CPTC 9 Dev Team Slides

What makes a CPTC?

- 48 Volunteers
- ~15k Volunteer hours
- 9 Development Teams
- Never enough sleep

What's new for this year?

Dev Team Updates

16 New Volunteers

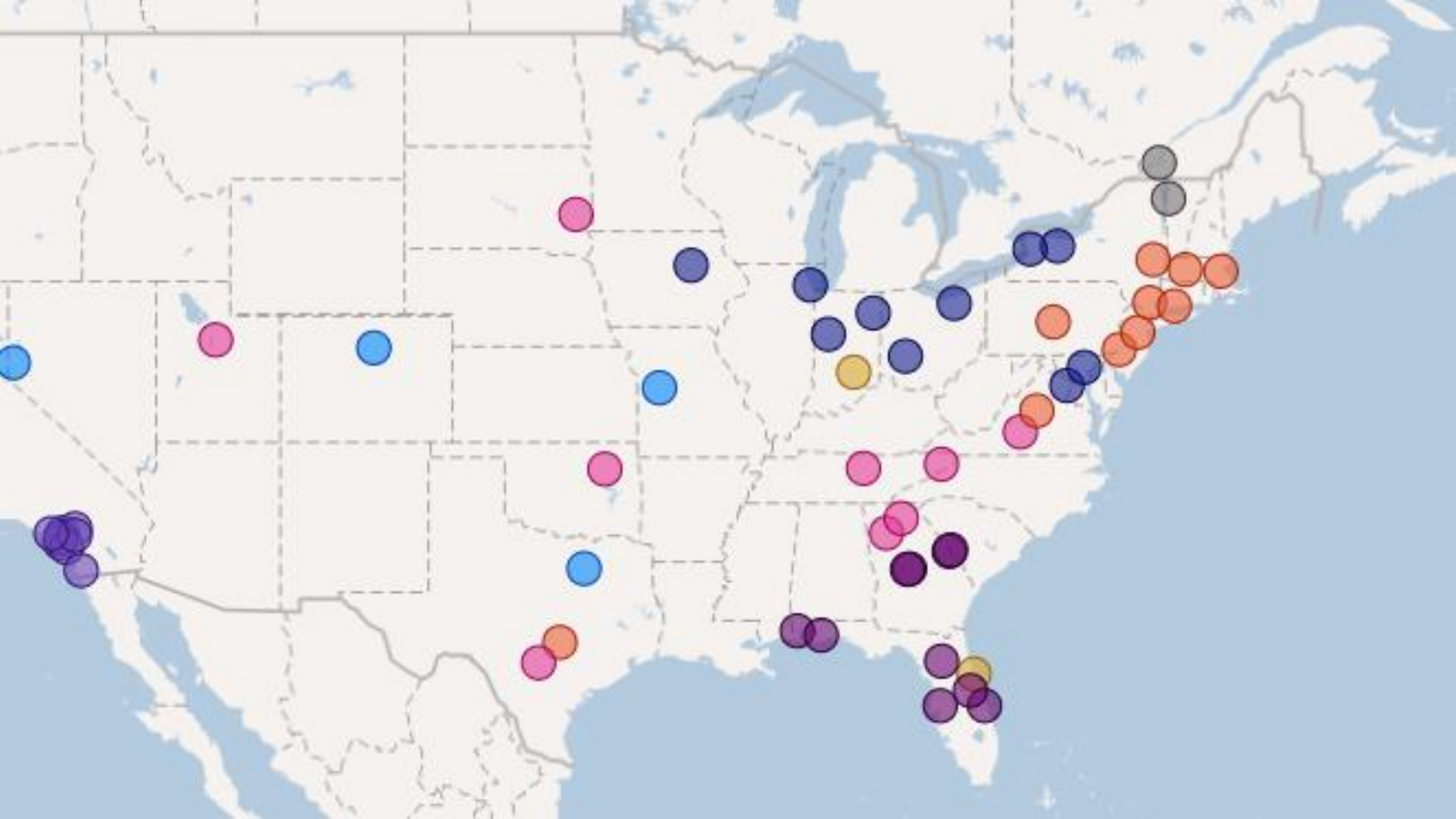
2 New Directors

22 New Teams

1 Google –> Microsoft Migration

A look back at #CPTC9

- @Meredith
- 8 Regional Events
- All US-based in-person regions filled



Infra

Infra

@AUSTIN

Infra

#Forrest bash magic. look away!!!

```
ssh-keygen -q -t rsa -N '' -f /root/.ssh/id_rsa <<<y >/dev/null 2>&1
cat /root/.ssh/id_rsa.pub >> /root/.ssh/authorized_keys
ssh root@127.0.0.1 -o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null -i
/root/.ssh/id_rsa -t "bash -l -c 'cd /tram-ops && bundle install && rake db:migrate'"
```

#ok you can come back.

Infra

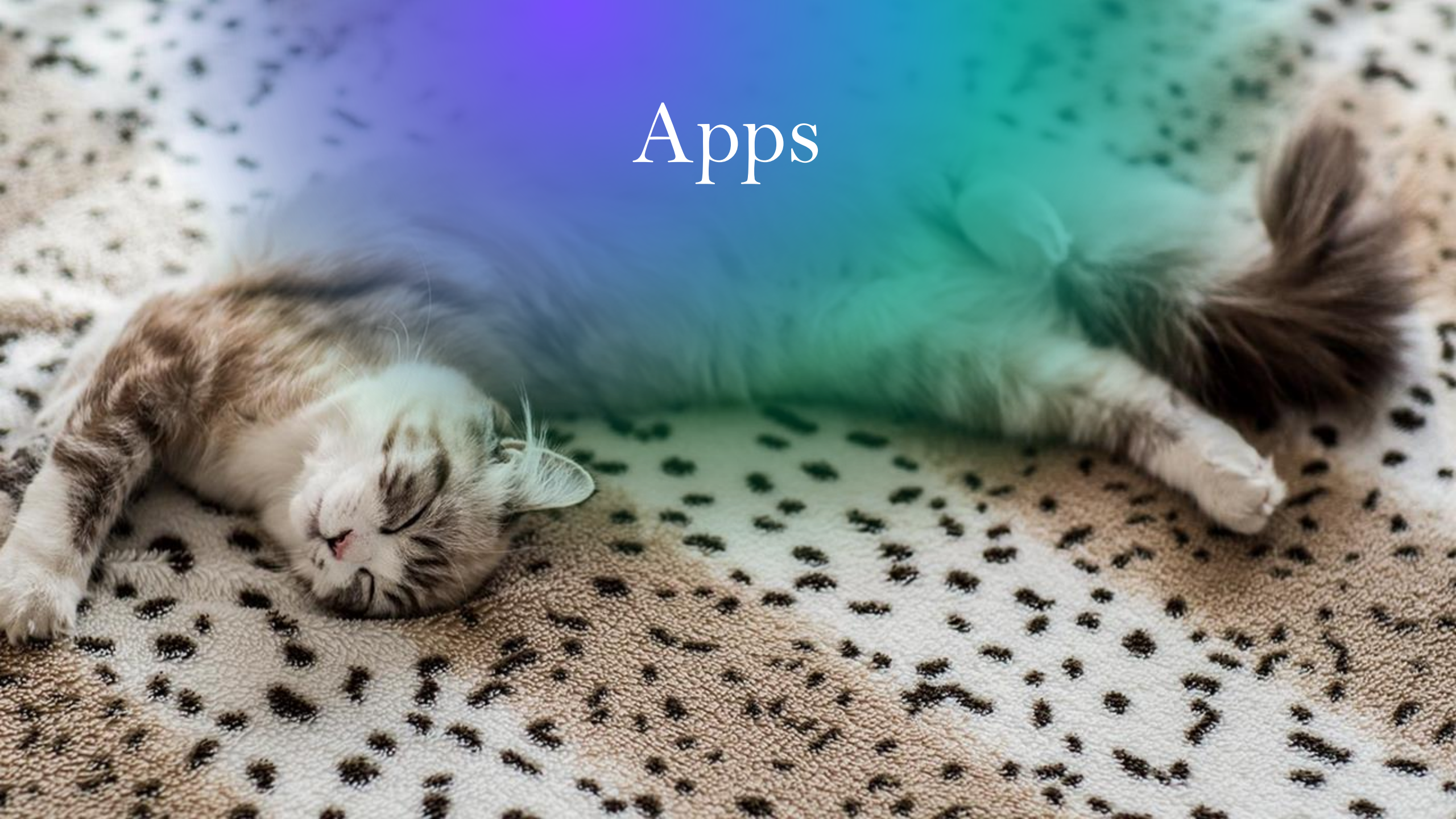
#Forrest bash magic. look away!!!

```
ssh-keygen -q -t rsa -N '' -f /root/.ssh/id_rsa <<<y >/dev/null 2>&1
cat /root/.ssh/id_rsa.pub >> /root/.ssh/authorized_keys
ssh root@127.0.0.1 -o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null -i
/root/.ssh/id_rsa -t "bash -l -c 'cd /tram-ops && bundle install && rake db:migrate'"
```

#ok you can come back.

RUBY IS BANNED ON INFRA

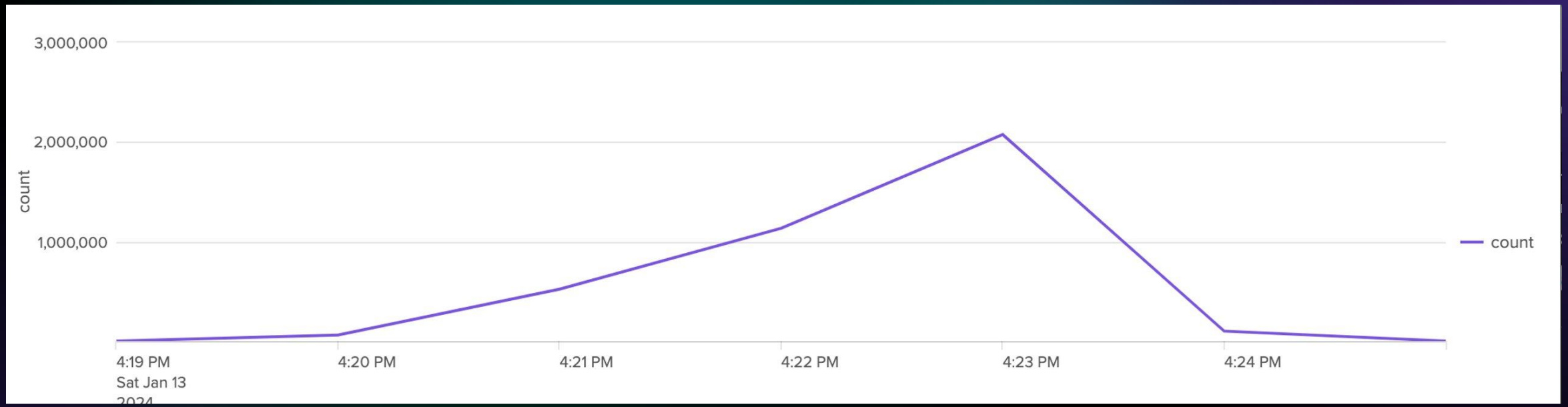
Apps



Apps

- Tram-Ops and Trams
  - Marshall
- TSA & Pilot PMI (Pilot Medical Information)
  - Jason
- Baggage Check-in
  - Gideon
- Flight Tracker
  - Izzie & Chris
- Employee Timecard / DB
  - Charles

Apps


3,000,000
2,000,000
1,000,000
count
4:19 PM
Sat Jan 13
2024
4:20 PM
4:21 PM
4:22 PM
4:23 PM
4:24 PM
count

Apps

time	hostname	cmd
2024-01-13 15:51:15 EST	vdi-kali01	ruby exploit.rb
2024-01-13 15:51:06 EST	vdi-kali01	nano exploit.rb
2024-01-13 15:51:03 EST	vdi-kali01	ruby exploit.rb
2024-01-13 15:50:24 EST	vdi-kali01	nano exploit.rb
2024-01-13 15:50:22 EST	vdi-kali01	ruby exploit.rb
2024-01-13 15:49:57 EST	vdi-kali01	nano exploit.rb
2024-01-13 15:49:53 EST	vdi-kali01	ruby exploit.rb
2024-01-13 15:49:16 EST	vdi-kali01	nano exploit.rb
2024-01-13 15:49:11 EST	vdi-kali01	ruby exploit.rb
2024-01-13 15:47:01 EST	vdi-kali01	nano exploit.rb

Apps

World

World

Robert A. Kalka
Metropolitan Skyport

Sock Accounts, Website, Phishing Content, Injects

- Greg
- Rachel
- Stuart
- Meredith
- Ian
- Tom
- Cathy

11ish Injects

21 fake employee profiles

24+ Pieces of OSINT

12 Polar Bears saved through RAKMS Charity Work

World

Robert A. Kalka

Metropolitan Skyport

Finals Injects.....

- Amazing Special Projects team injects!
- For other injects, emphasis on strategic thinking and business skills
  - Threat Prioritization RFI
  - AI Applications Presentation
  - GPS Spoofing Engagement Proposal
  - SME engagement (AWS Environment, Mitigation Review)
  - Rogue Interns!

Special Projects

Special Projects

The Special Projects Team makes small, cool things to add additional flavor to the world laid out by the Infrastructure and Apps teams!

Team Members & Projects:

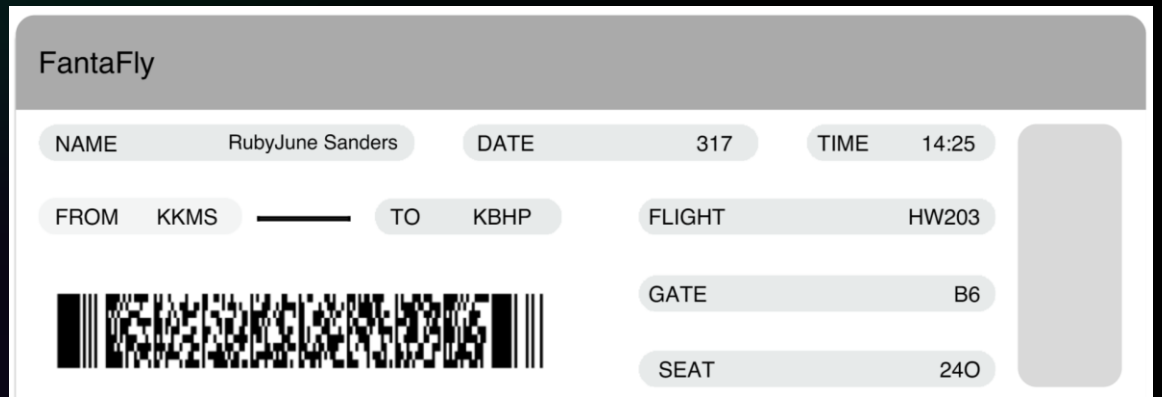
- Dan – Orchestration & AWS design
- Jasmine – Boarding Passes & Barcodes
- Joe & Forrest – RF Baggage Claim
- Matt & Jennifer – Airport Map, Tool Ordering, Fox Hunt

AWS Challenge – Boarding Passes

kalka-passes / rakmsbarcode
AWS S3 and Lambda

Jasmine
Discord handle: cofine#6069

- Publicly accessible S3 bucket with dummy data boarding passes
- Lambda based PDF417 barcode generator for boarding passes captures PII without any particular safeguards or controls
- Inspired by the Tony Abbot boarding pass event – Australian PM posted picture of boarding pass on Instagram and it had his passport number in it
- Custom generated boarding pass barcode + boarding pass template = MAJOR security issue



AWS Challenge – Airport Map

rakmslocationservice

AWS S3 and Lambda

Matt & Jennifer

- Based on Bluetooth beaconing indoor location systems
- API only but basically walks you through how to exploit it
- Can exfiltrate all of the beacon info via the API or as a hidden layer in the map SVG
- Location data includes sensitive areas without any authentication – can enumerate the entire map database including TSA, Alstom Cityflo Control Room, EOC, Confiscated Weapons Storage, and the CPTC Server Room

AWS Challenge – Tool Ordering

rakmstoolrequisition

AWS S3, Lambda, DynamoDB, Rekognition

Matt & Jennifer

- AI is everywhere, so why not use it for ordering tools too!

- Images of all valid tools are in a folder leaked in the HTML
- Lots of data leaks in error messages – PNG or non-tool images, zero quantity, etc.
- Easter egg if you uploaded a picture of a pet animal
- No access restrictions (world accessible)
- "Photo" auth for big purchases doesn't do any liveness checks and a photo that will work is in the leaked demo items folder
- Quantity limits aren't checked server-side
- Nothing pairs the recognized tools to the finalized purchases, so requisition database is enumerable and finalized without having made the initial request

IRL Exercise - Fox Hunt

- Tasked cross-team groups to work together to locate a source of radio interference.
- "Foxes" were low-power ham radio transmitters hidden in various areas of the building.
- Groups were given a radio receiver tuned to their beacon with a slightly directional antenna.

- All groups found their beacon! Fastest group was 8 minutes, others were around 30 minutes.
- Cross-team task, a first for CPTC!

RF Analysis Challenge – Baggage Claim

```
Manual Transmission IDC 28405
Team Number: 5
Message Type ID: 48
Message Packet(
    Channel=5
    Message Type=48
    Separator=False
    Nested=False
    Message Size=9
    Current Time=1704848777
    Update Time=1704848777
    Temperature=55
    Status=C
    Message=TEST 1234
    Format(
        SOM=809648455
        Separator=59
        EOM=1111574320
    )
    Packet Size=40
)
RAW Bytes:
    30 42 41 47 05 30 3B 09
    43 65 9D ED 89 65 9D ED
    89 00 37 54 45 53 54 20
    31 32 33 34 00 00 20 5B
    42 41 47 30 00 00 00 00
```

WASABYTE

Joe (wasabi) and Forrest

100% Custom Python Software send and receive packets

Utilizes CC1101 Chipset via SPI Bus allowing for ~64-128 byte average messages a second

Had an api service (bccs), had a transmitter (bctx), and a reciever (bcrx)

Message encoded in bytes and bits, utilizes bit shifts and other tricks. Completely dynamic.

Live weather reports thanks to OpenWeatherMap

Kali Laptops – Preloaded with GNU Radio, RTL433, and Universal Radio Hacker

Each team given a RTL SDR, Basic instructions, and access to the transmission page

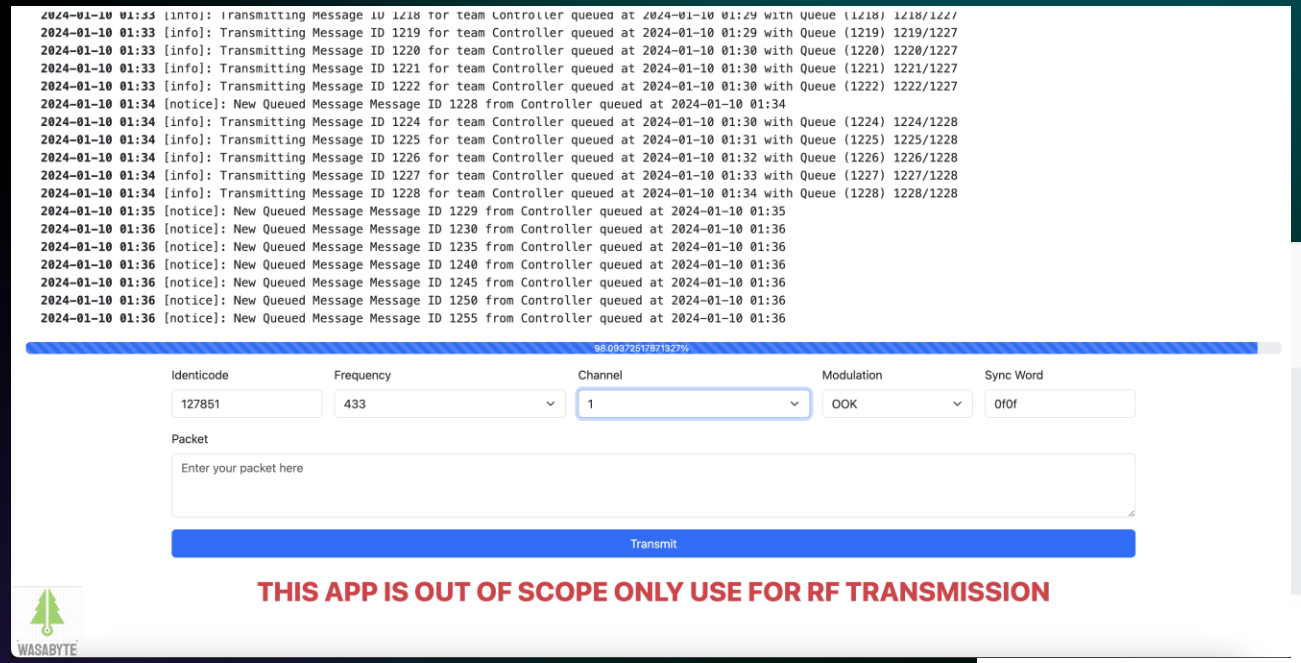
Transmitter page let teams transmit anything as bytes

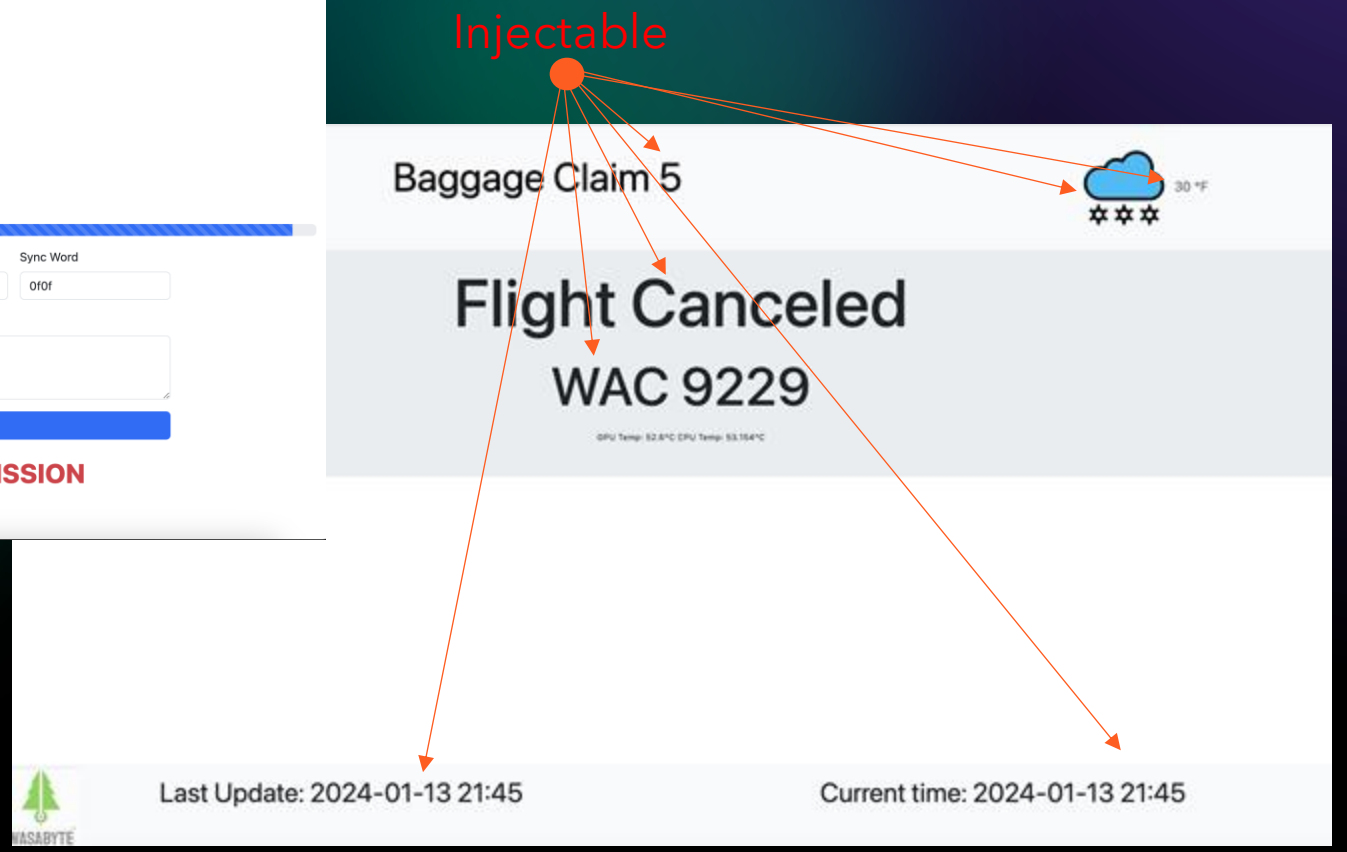
Forrest and I spent several days over Christmas ensuring teams could properly use this challenge

Challenge was meant to be challenging. But open to suggestions

How much did you find?

Transmission and Status Pages





Comms

Comms

- 239 total tickets during competition hours
- 50+ scheduled/automated emails during the events to support injects
- 1161 total tickets this season

Monitoring

Monitoring

Our Jobs:

- Splunk Engineering (Infra Setup, Data Ingestion)
- SOC
- Threat Hunting
- SOAR Automation and Receipt Printing

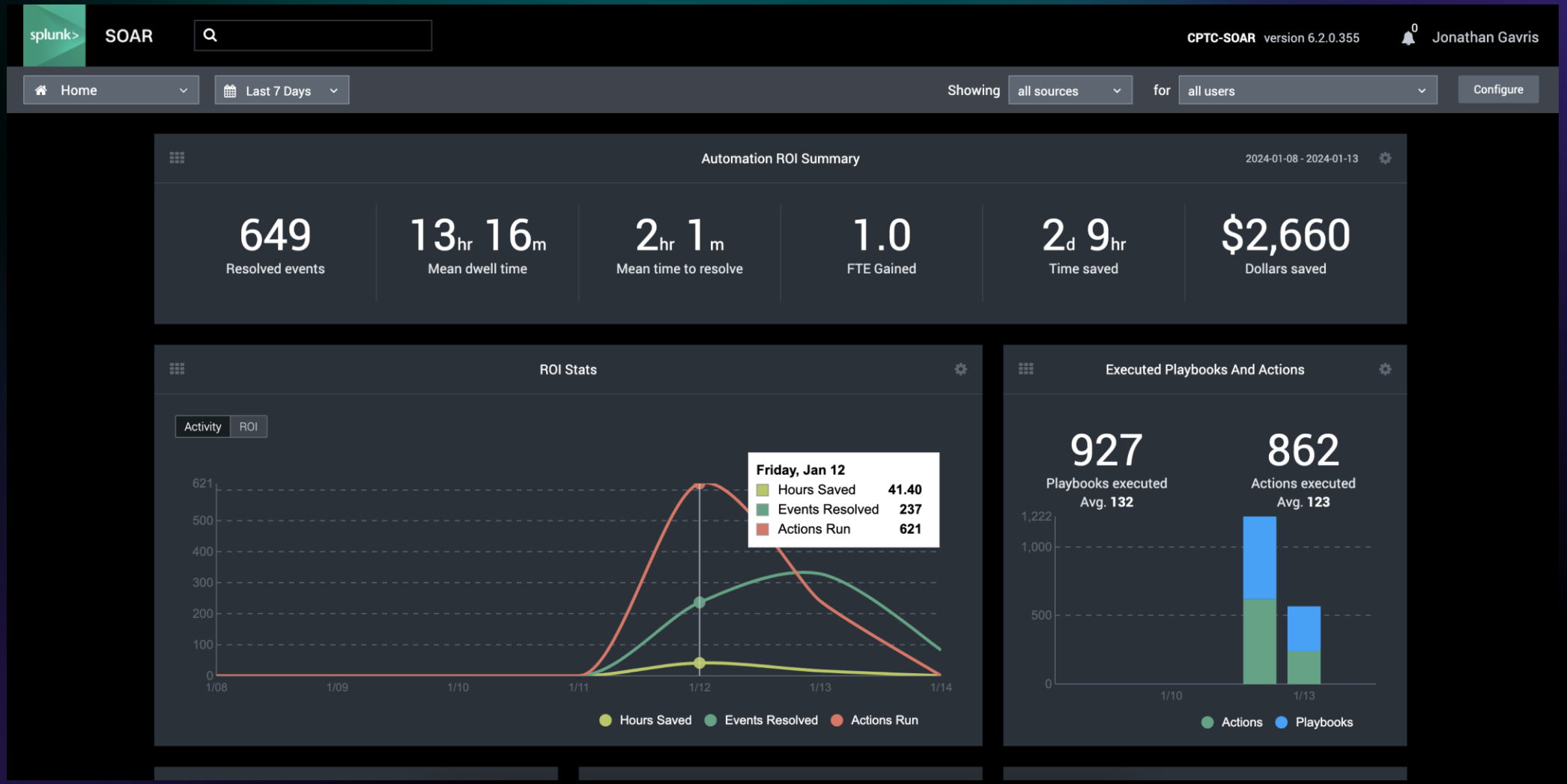
Quick Statistics:

- Ingestion Volume: 476 GB
- Command Tracking: 40000+

Command Statistics

cmd_root	team_count	total_count
ls	15	6673
cd	15	3781
aws	14	3770
nmap	15	2130
cat	15	1600
curl	15	1289
clear	14	1172
nano	15	1087
crackmapexec	13	957
ffuf	10	838
git	15	738
nxc	2	708
vim	11	674
sqlmap	11	595
apt	15	531
ssh	15	506
gobuster	13	469
evil-winrm	13	388
proxychains	8	385

Alert Handling



Directory Brute Force

- Teams love directory brute forces
- A team used ffuf to generate 9M+ requests to Baggage Checkin Apps

cmd	team_count	total_count
ffuf	10	838
gobuster	13	476
hydra	11	278
dirb	8	239
wfuzz	8	140
feroxbuster	3	128
dirsearch	3	104
dirbuster	6	27

Others

```
echo "canSPlunkkkkkKKadminsssseeee this??? mwahaaaaaaaaaaaaaaaaaaaaaaaaaa"
```

```
echo "Your response time was fast for that one message on VDI #3. Take care, SOC folks."
```

Others


Team-User Agent
CPTC9-Finals-t1-corp-baggagecheckin
CPTC9-Finals-t2-corp-baggagecheckin
CPTC9-Finals-t3-corp-baggagecheckin
CPTC9-Finals-t4-corp-baggagecheckin
sqlmap/1.8.1.4#dev (https://sqlmap.org)
Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0)
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

New Detection!

Correlation Search

Search Name

CPTC Potential ZeroLogin

App

Enterprise Security

App Context

Enterprise Security

Set an app to use for links such as the drill-down search in a notable event or email adaptive response action. If set to None, the setting defaults to the current application context.

Description

Looks for computer account password changed.

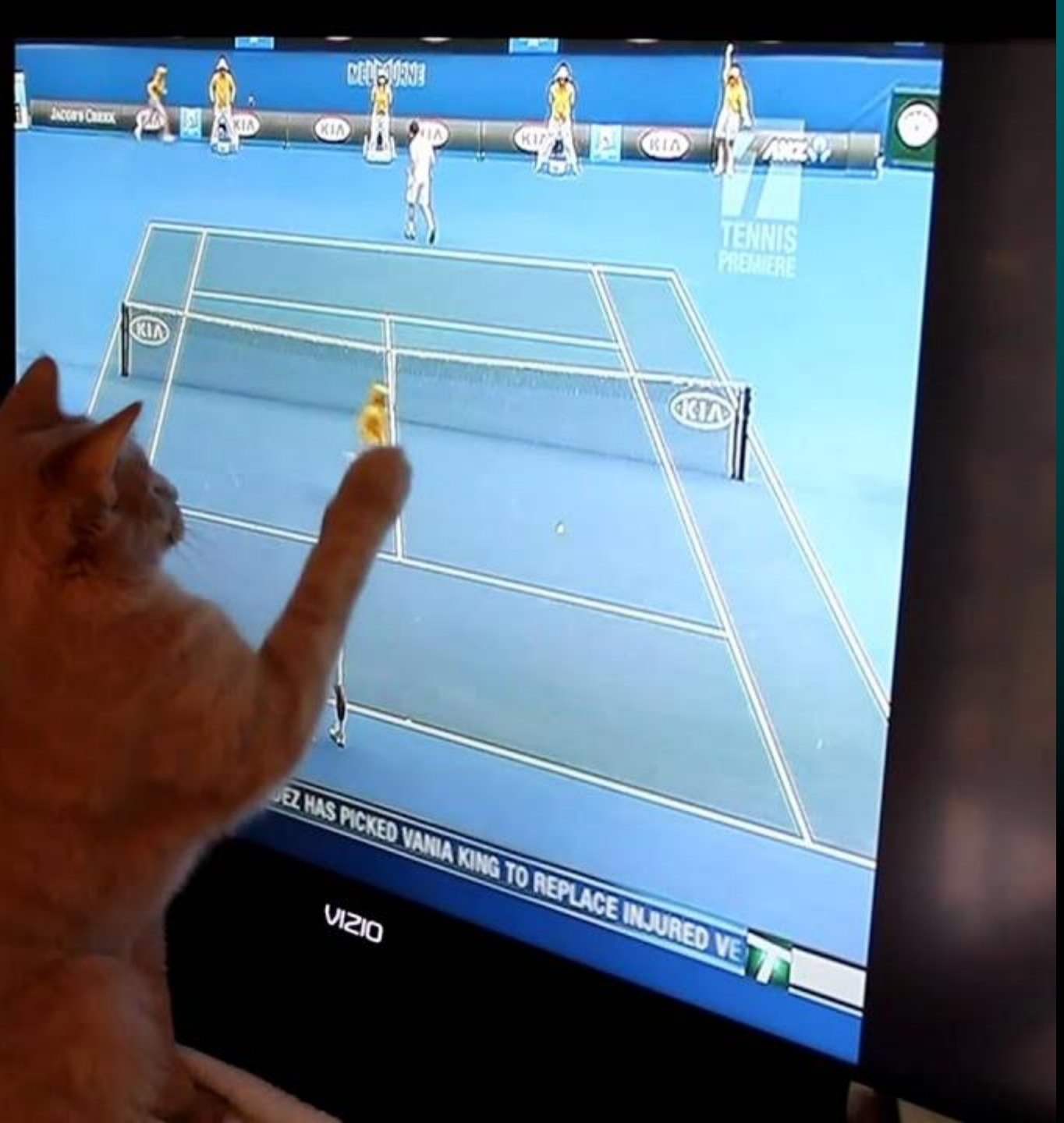
Mode

Guided | Manual

Search

```
index=windows_security EventCode=4742  user=*$ NOT PasswordLastSet="-" src_user="ANONYMOUS LOGON"
| stats values(EventCode) as EventCode values(name) as name values(PasswordLastSet) as PasswordLastSet count by src_user user host
| `cptc_get_team_from_host(host)`
| rename host as orig_host
```

Scoring



Scoring

- @Stuart
- Jason – talk about redaction
- This was the year of educational opportunities
- Key takeaways for teams

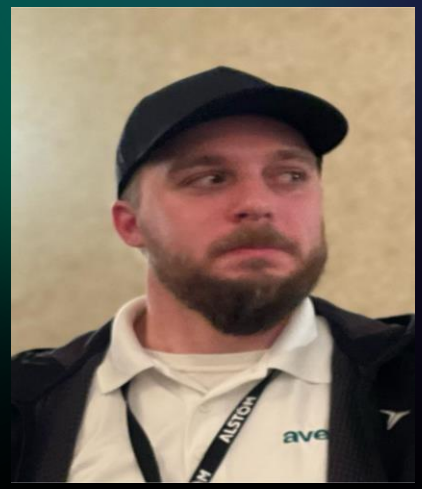
Engagement

On a Scale of Stuart to John How Do You Feel Today?

Did I Even Wake Up?
-Stuart

This Is The Flavor of Life
-Dan

What Was The Question Again?
-Raul



I Need Emotional Support
-Austin

But Did You Die?
-John

Do It For The 'Gram:

- Follow us on LinkedIn and Twitter for all the latest updates
- SURPRISE! Photos will be getting added to the website within the next few weeks.(CPTC 8-CPTC9) We will post to social media to announce.
- YouTube- Upcoming Panel Alert
  "Unveiling the Professional Journey of Collegiate Penetration Testing Rivals turned Volunteers"

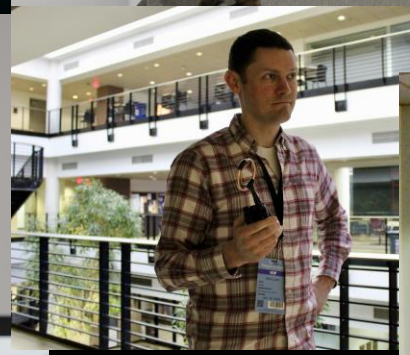
This is Our Inclusion Era:

- This year has been a historic year for CPTC. We have the highest number of Female identifying Competitors, Coaches, Volunteers, Staff, and Sponsors.
- According to most recent Women in Cybersecurity (WiCyS) report Women make up only 24% of the Cybersecurity work force.
- We will be working this year to gather resources to help with recruitment and retaining of diverse teams.

What About The Coaches?

Banquet Networking

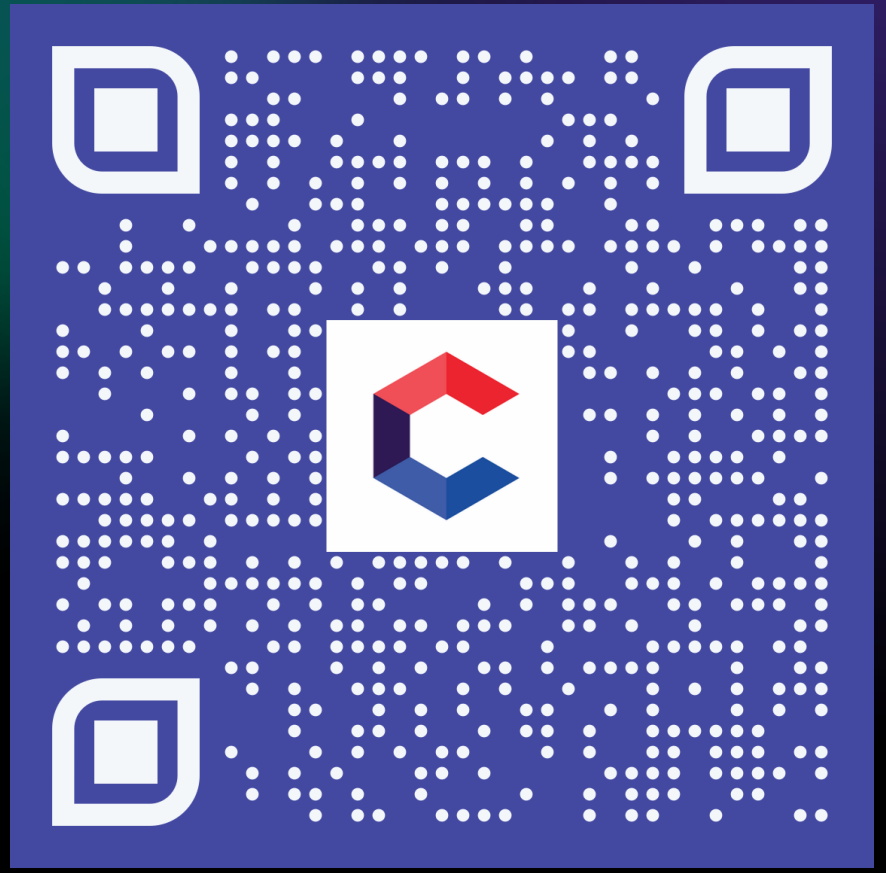
Coach Talks with Alex Levinson,
Head of Security at Scale AI



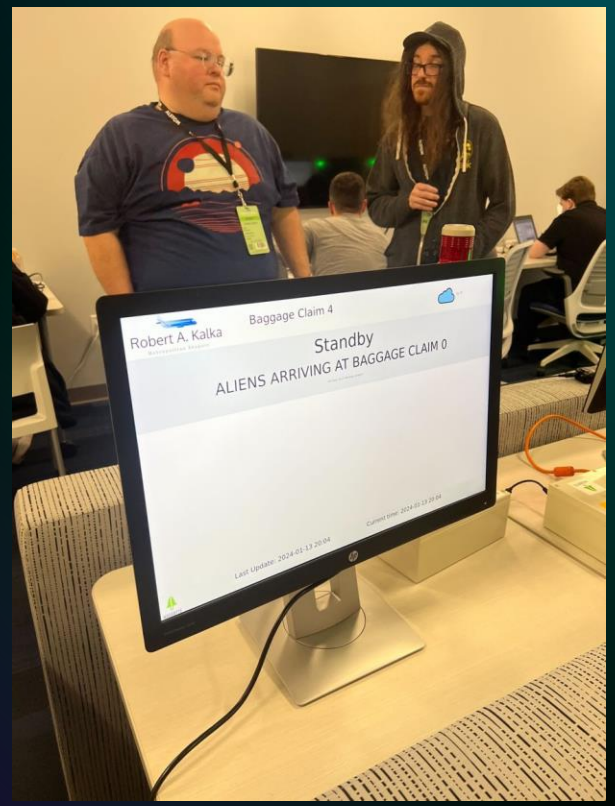
Coaches
Fox Hunt

We Want to Hear From You?

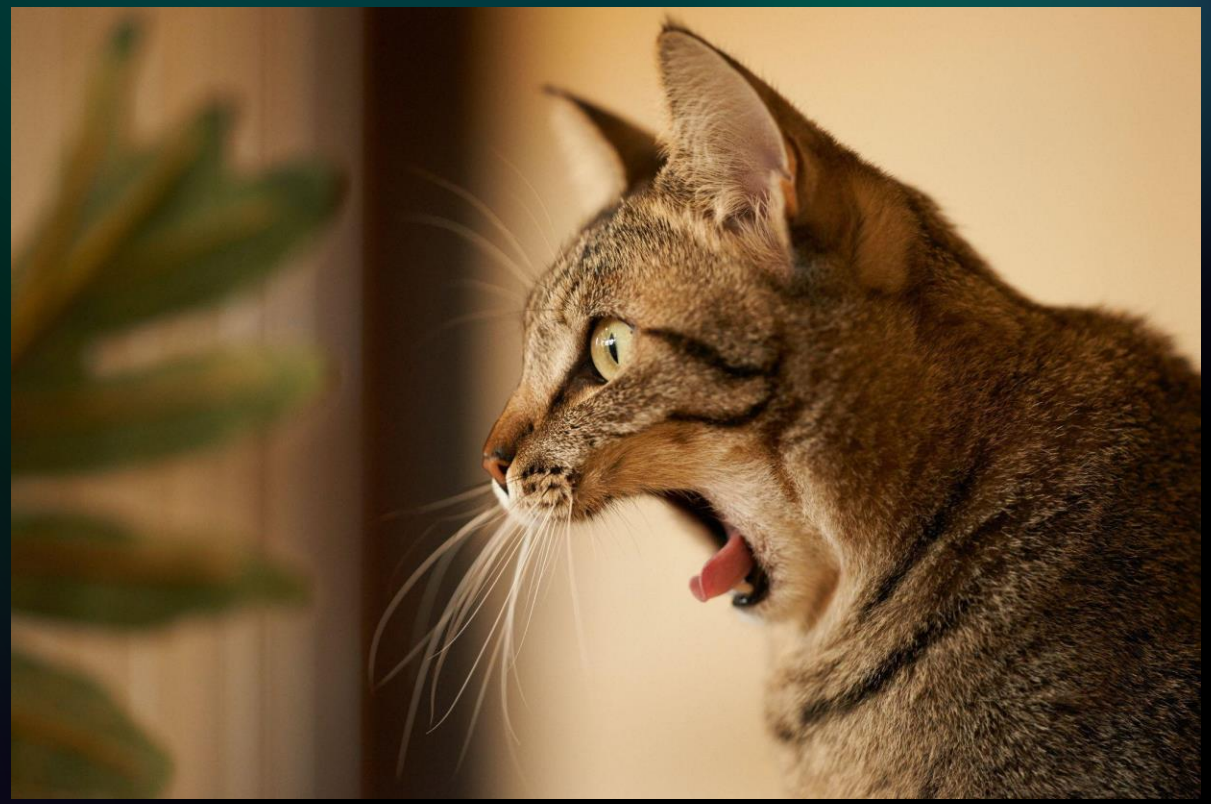
Calling all participants of the Collegiate Penetration Testing Competition! We invite you to share your valuable insights by completing a brief student survey, helping our staff enhance the competition experience for future participants.



Fun stuff we saw



Scary stuff we saw



VM and Log Export

Researchy stuff

bit.ly/48zKbXW

https://rit.az1.qualtrics.com/jfe/form/SV_0TdS7hcbWAPmcpo