2019 Dev Overview

November 24, 2019


Crowe

Monday, October 21st

lucas 11:45 AM
Image from iOS

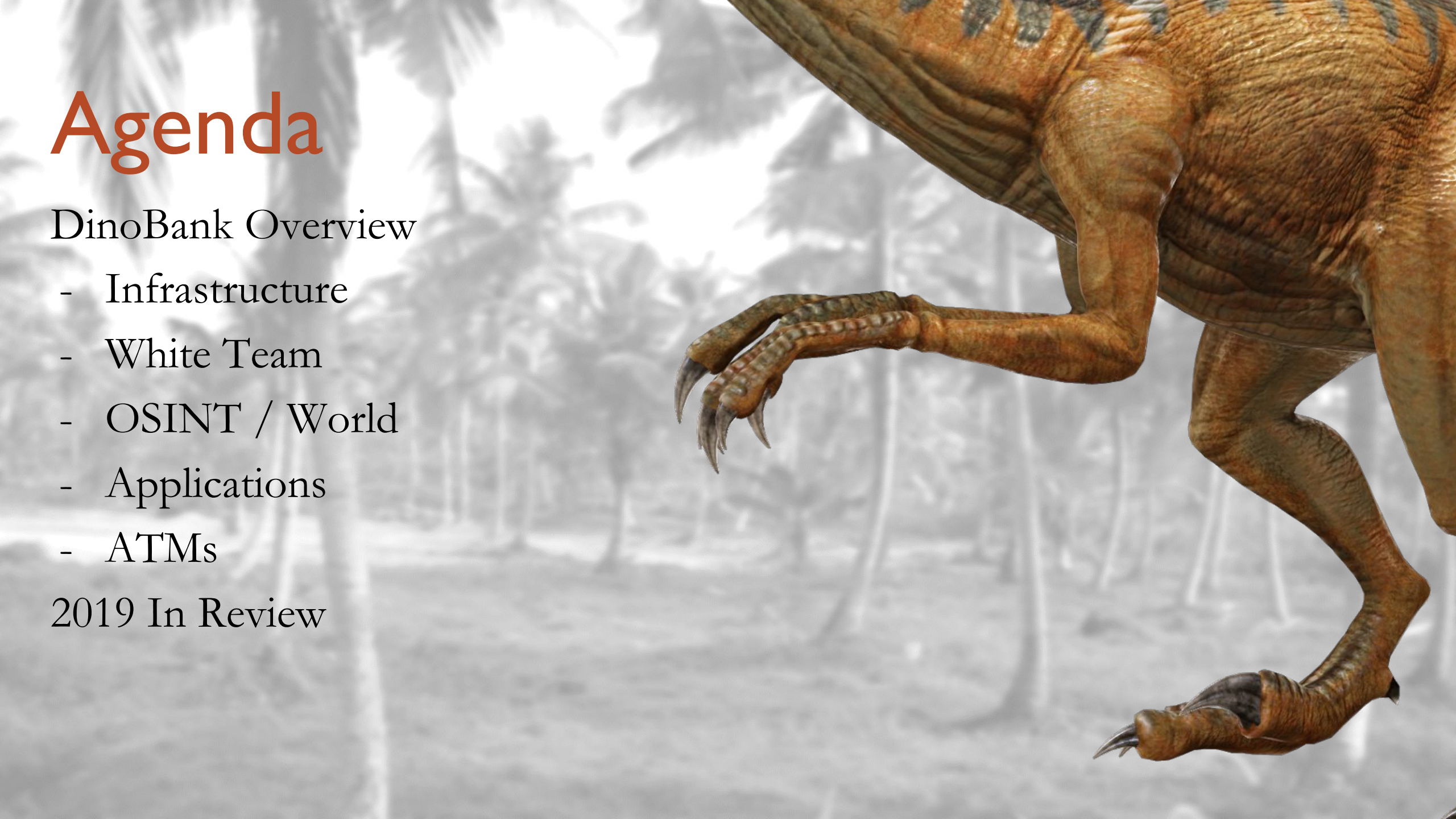
Tom and I may have to go half way across the country to run into each other, but I wanted to make sure everyone knew our breakfast was that of 'des champions'

Agenda

DinoBank Overview

- Infrastructure
- White Team
- OSINT / World
- Applications
- ATMs

2019 In Review

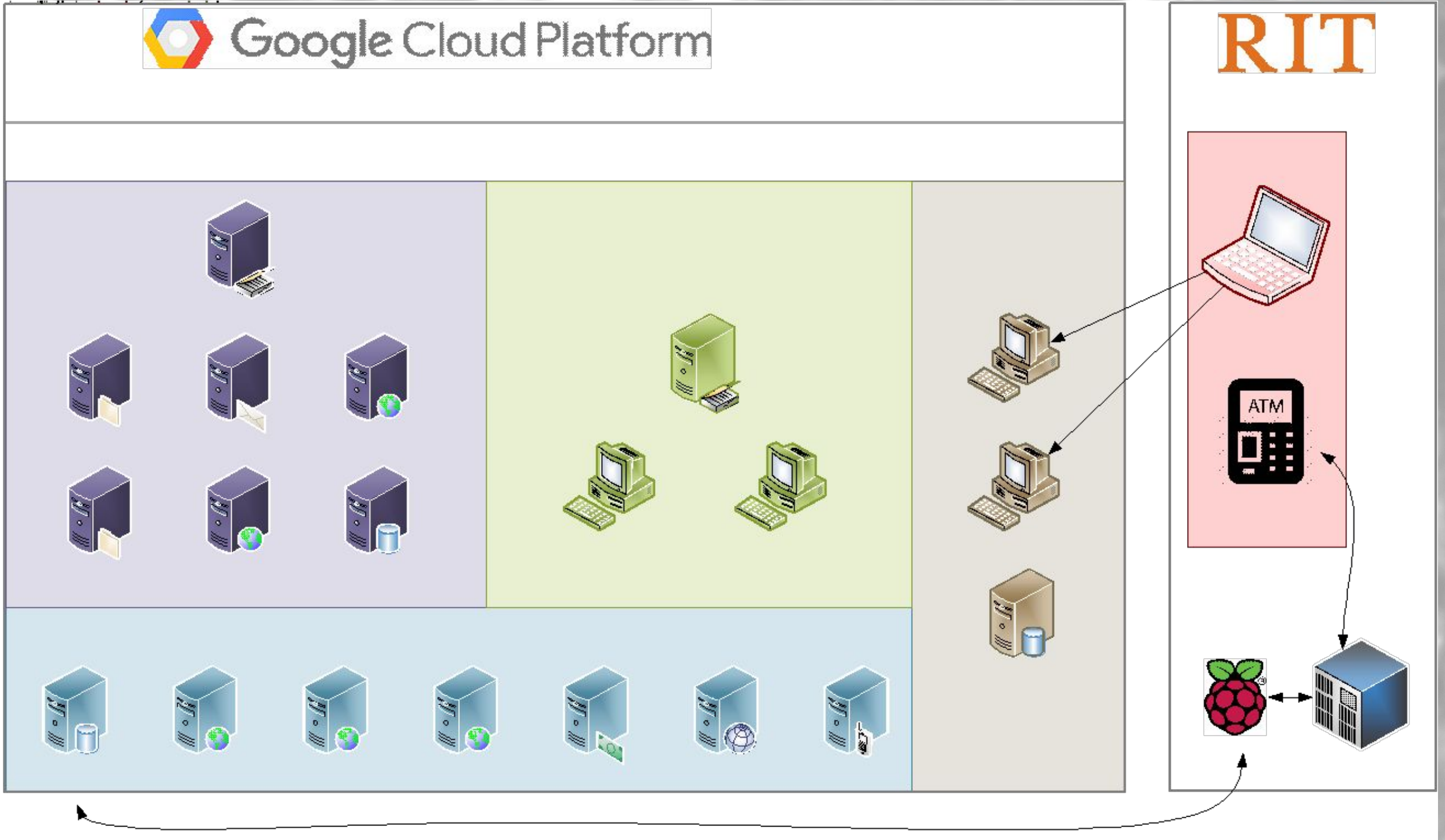


DinoBank Overview

- New Black Team Structure
  - More volunteers
- Bigger environment
  - 18% more hosts
  - Double the lines of code in apps
  - Coins and ATMs!
- Full environment at regionals
- More interactions and OSINT
- Deployed early!
  - But had to cut some hosts at regionals

Infrastructure

Lucas Morris


Google Cloud Platform
RIT
ATM

White Team

Tom Kopchak

Tom Kopchak @TomKopchak · Oct 2

College students are incredibly effective e-mail generators.

3 1 9

Twitter is fun

Burner Herzog @DJHardB · Oct 8

If @nationalcptc is aiming for authenticity/realism, they certainly knocked it out of the park on this one...

Q. Have you implemented a disaster recovery plan?

A. We have been planning on creating one for at least the past 65 million years.

1 8 21

White team deliverables

- 6 simultaneous regional events
  - 4 time zones
  - 2 countries
- One consistent story line
- Scheduled e-mails
- Planned presentations
- On-the fly changes
- Volunteer/sponsor interaction
- Coordination with black, world, and monitoring teams
- Approximately 22 million emails

Interactions

to me

Dear Mr. Dickson,

We would like to report an incident of vandalism that occurred over our lunch break. At some point while we were away, an individual entered our room without authorization, erased our whiteboard, unplugged our mice and network cables, and wrote "10.0.1.115 - WHAT THE HELL IS HE DOING?" on our board.

to me

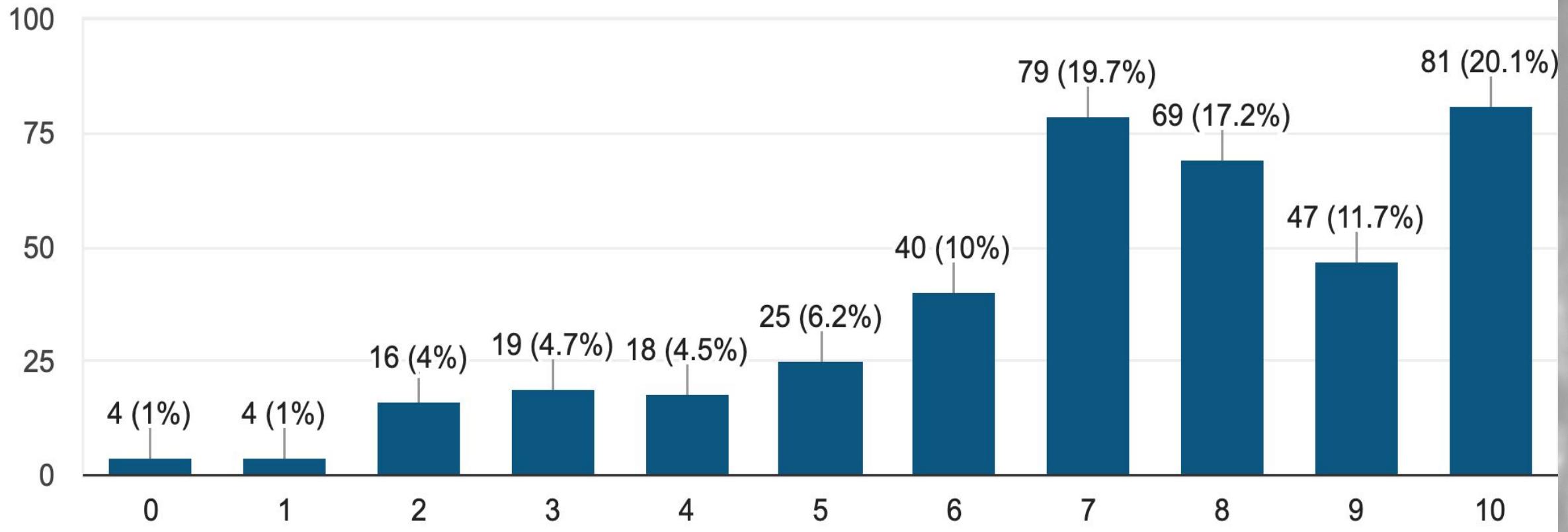
Hi Tom,

We received a request from the CEO to pair his garage door opener to his new Mercedes by the end of the day. We do not believe this is in our scope of work. Please confirm this as a new element of the scope.

Sincerely,

Score

402 responses



OSINT / World Team

Dan Borges

OSINT

r/DinoBank

Search r/DinoBank

Posted by u/lawrence_hayden 25 days ago

2

Is anyone else's computers running slow?

My computer has been running slow, and apparently others are as well. Has anyone else had this experience? I have been told this is fine and there is nothing to worry about. I wouldn't think new computers would run this slow!

3 Comments Share Save ...

Posted by u/dino-alex-faulkner 28 days ago

1

Wow found some instances of "Password1" on our workstations! Thankfully we found and fixed that asap!

Wow found some instances of “Password1” on our workstations! Thankfully we found and fixed that asap! — Alex Faulkner (@AlexFaulkner17) October 27, 2019 from Twitter https://twitter.com/AlexFaulkner17

from Tumblr https://ift.tt/2JpRlEq

Comment Share Save ...

Posted by u/dino-alex-faulkner 1 month ago

1

Mmmm some amazing food at the Crispy Croissant in our Gotham branch

Mmmm some amazing food at the Crispy Croissant in our Gotham branch — Alex Faulkner (@AlexFaulkner17) October 4, 2019 from Twitter https://twitter.com/AlexFaulkner17

OPEN SOURCE INTELLIGENCE

After traversing through crafted Google searches, we discovered a lot of information about high ranking DinoBank employees.

- Cale Strickland - Operations
- Dahlia Dawson - Compliance and Ethics Officer
- Mauren Davenport - Information Security Officer
- Meredith Sournoise - Director Marketing Communications
- Alex Faulkner - Chief Information Officer
- Dan Oliver - Compliance Department Director
- Ruth Brooks - Bank Secretary Act
- Lawrence Hayden - Chief Executive Officer

Employees at DinoBank

Cale Strickland
Operations at DinoBank

Dahlia Dawson
Compliance and Ethics Officer at DinoBank

Mauren Davenport
Information Security Officer at DinoBank

Meredith Sournoise
Director Marketing Communications at DinoBank

Totally Legit Human's job update

Totally Legit Human • 1st

System Analyst at Asteroid Bank, but also the world's most loyal custom...

3d

Congratulate Totally for starting a new position as System Analyst at Asteroid Bank

Like Comment

Congrats Totally | Happy for you! | Congrats! Let's catch up

Be the first to react

WORLD

Saturday	8:55 AM	9:15 AM	Pulled	Board/Runner	Board meetings with teams
Saturday	9:10 AM	9:35 AM	In person	Dax Whitney	Wtf are you doing to our network?
Saturday	9:25 AM	9:50 AM	In person	Paul	how can you make us unhackable?
Saturday	9:35 AM	10:00 AM	In Person	Alex Woods	Touch base, seed the undermining of Tom
Saturday	9:50 AM	10:15 AM	In Person	Tom Dickson	Hows the pentest going? Can I get you anything?
Saturday	10:00 AM	10:25 AM	In person	Alex F	Visit teams, cause additional chaos
Saturday	10:10 AM	10:35 AM	In person	Preceous	This is really important to us, lots of jobs are on the line
Saturday	10:25 AM	10:50 AM	In person	Hilary Mathis	Visit from Legal Counsel
Saturday	10:40 AM	11:05 AM	In person	Johnathan Gay	Hey IT guys, I have a question. I have this really useful program that I used to use back in 1995. I want to install it on my comp
Saturday	10:50 AM	11:20 AM	In person	Krissy Duval & Bobbie Mooney	First auditor visit
Saturday	11:00 AM	11:30 AM	Email - se	Tom Dickson	WTF Alex?
Saturday	11:05 AM	11:45 AM	In Person	Jacquline Woods	Downplay audit
Saturday	11:20 AM	12:00 PM	In Person	Dan Oliver	Visit Teams, super pleased with the audit so far
Saturday	11:30 AM	12:15 PM	In Person	Mauren Davenport	I'm writing a company letter for this week and I want to put some info about this as this seems like a really important thing. Can
Saturday	11:45 AM	12:30 PM	In person	Alex F	Visit teams, even more chaos
Saturday	12:00 PM	12:45 PM	In Person	Meredith	I just got a spam email. I thought you are supposed to make us secure! Are you even trying?
Saturday	12:00 PM	1:00 PM	Email -ser	Tom Dickson	ATM/IVR Issues?
Saturday	12:15 PM	1:15 PM	In Person	Ali Gamble	You do know the higherups won't actually do anything about this until next quarter, right? They're super stingy with money and
Saturday	12:30 PM	1:30 PM	In person	Alex Woods	ATM Issues
Saturday	12:40 PM	1:45 PM	In person	Dax Whitney	IVR issues
Saturday	1:00 PM	2:00 PM	In Person	Krissy Duval	Audit Checkup
Saturday	1:10 PM	2:15 AM	In Person	Lawrence Hayden	Hey! I can't get the printer to work. Do your job and help me now or I'll get you fired.
Saturday	1:20 PM	2:30 AM	Pulled	Alex F	An immense amount of chaos, leave teams leaderless for the PII email
Saturday	1:30 PM	2:45 AM	Email	Tom Dickson	Customer/Employee PII

Insider Threat

FINDING #	20	TITLE	Indicator of Compromise - Malware		
RISK	INFO	IMPACT	INFO	LIKELIHOOD	INFO
HOSTS	10.0.10.201, 10.0.10.202, 10.0.10.203, 10.0.10.208, 10.0.10.209, 10.0.12.201, 10.0.12.208				

DETAILS

In the Windows machines listed, [redacted] found a binary "miner.exe" in the "C:\Windows\System32" that was not running. Upon further investigation, [redacted] discovered that this binary was a cryptocurrency miner. [redacted] considered this a potential indicator of compromise and immediately contacted the point of contact. [redacted] was notified that cryptocurrency miners are unauthorized and was asked to conduct a further investigation.

Furthermore, during the course of our engagement, [redacted] discovered an email chain around 10/06/2019 where Dan Oliver instructed Alex Faulkner to remove a cryptocurrency miner that Faulkner had installed on DinoBank machines.

MITIGATION

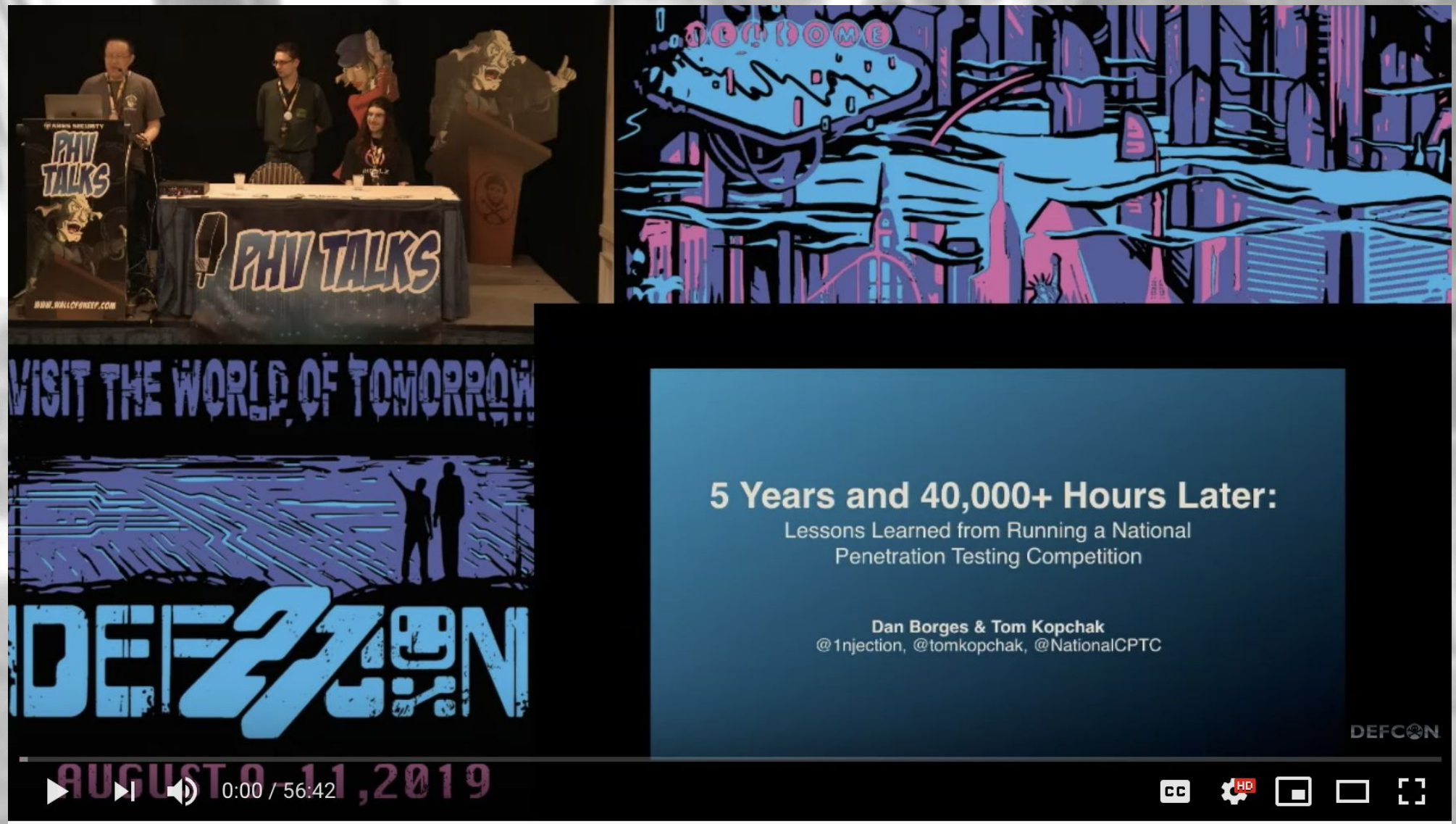
Ensure that the cryptocurrency miner is removed from all machines and perform an audit for further malicious threats that may be present in DinoBank's environment. [redacted] does provide this service should DinoBank be interested in pursuing future engagements.


Information Security
Alex Faulkner
Chief Information Officer
DINOBANK
Information Technology
George
Chief Morale Officer
DINOBANK
DINOBANK
STAFF

A word from Tom Dickson

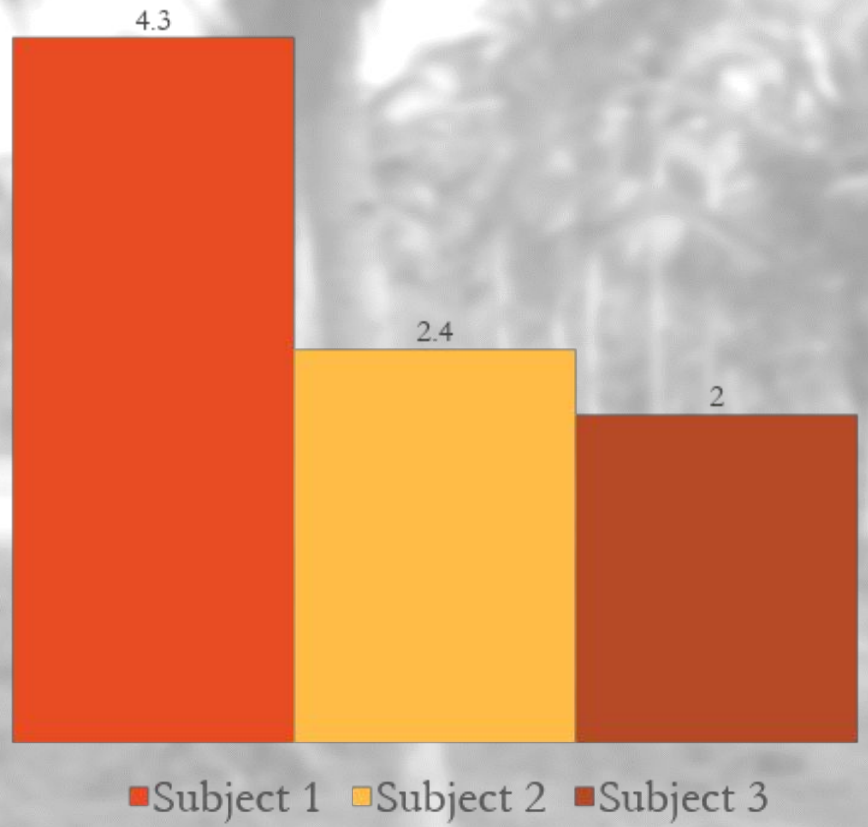
- Tips when talking to the board

OSINT on the CPTC!



DEF CON 27 Packet Hacking Village - Tom Kopchak - Lessons Learned Running a Pentesting Competition

Data / Observations

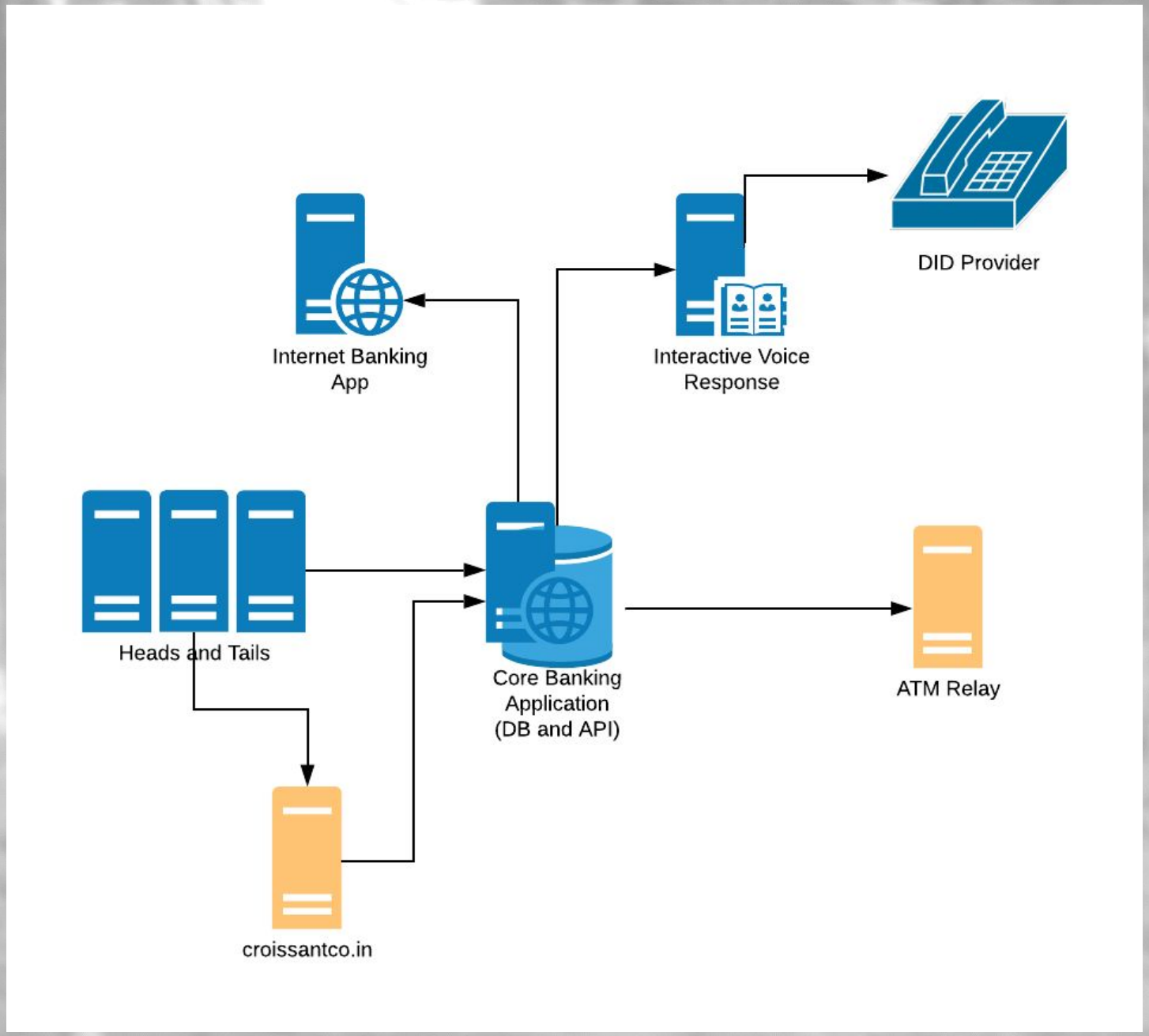


Use the Chart feature to quickly show differences between results.

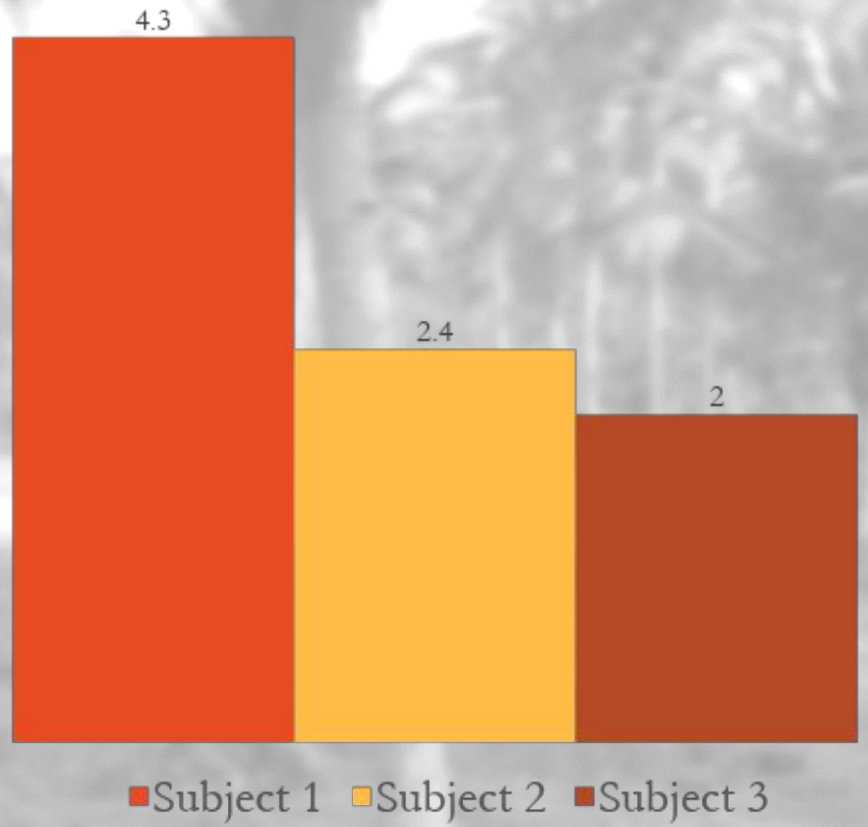
Under the Insert tab, look for the Chart button or simply click an empty placeholder text box and choose the display style that suits your needs.

Application Team

Jason Ross


DID Provider
Internet Banking App
Interactive Voice Response
Heads and Tails
Core Banking Application (DB and API)
ATM Relay
croissantco.in

Data / Observations



Use the Chart feature to quickly show differences between results.

Under the Insert tab, look for the Chart button or simply click an empty placeholder text box and choose the display style that suits your needs.

ATM Skunkworks

Forrest Fuqua

Joe Needleman

You probably noticed some ATMs...


R·I·T
Dubai
4759 3288 1585 0615
DINO BANK
NEVER PREHISTORIC
Team 1: RIT

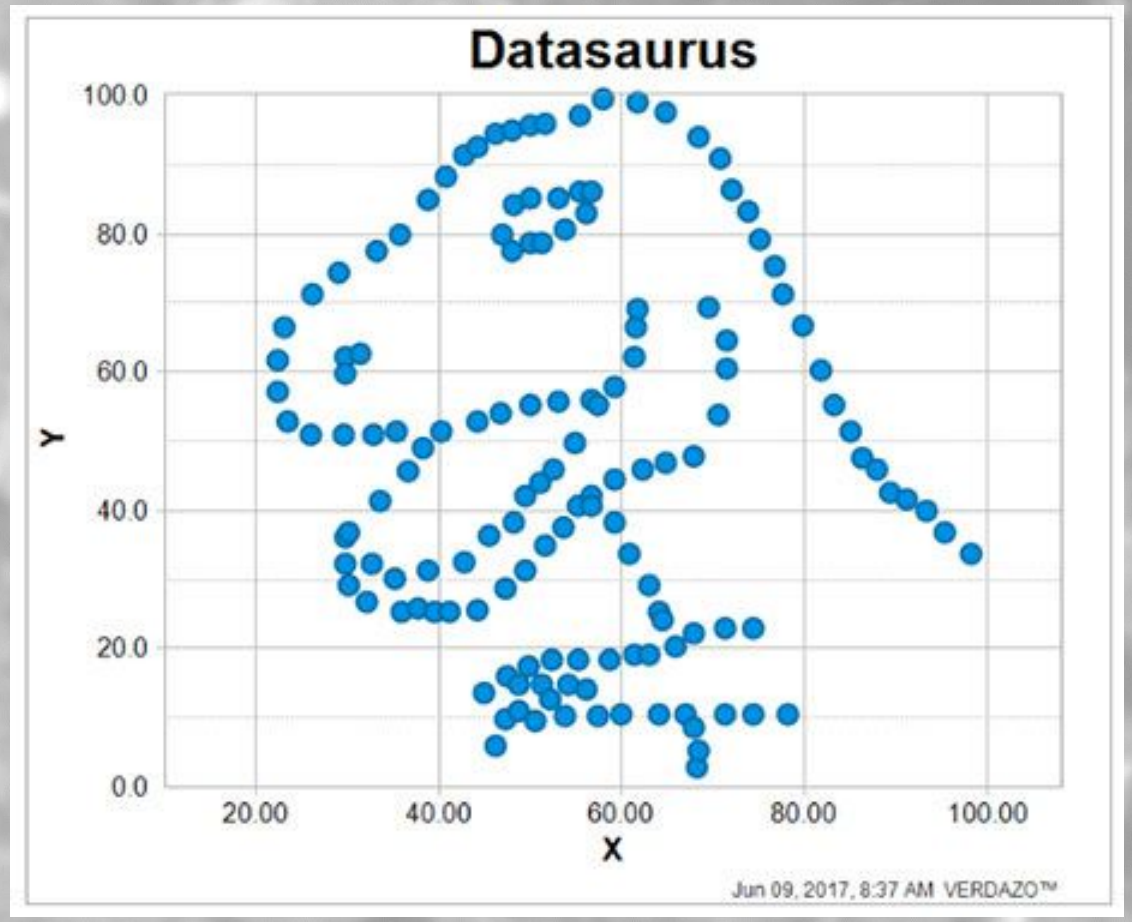

MINI-BANK
REJECT BIN
EXIT
B-SIDES TDX
THE HACKERGROUND
VIRUSTOTAL
fsociety
I DO NOT CONSENT TO THE SEARCH OF THIS DEVICE

Mass Extinction

DinoBack with a thorough penetration test report.

Statistics

- #### commits
- ~11,000+ hours of dev time
- ### lines of app and script code
- ~13.3 TB of total log data
- ~22 TB of research data
- ~$32,000 cloud spend
- $3,000 on eBay
- 6 full hours of sleep (per person) Friday!



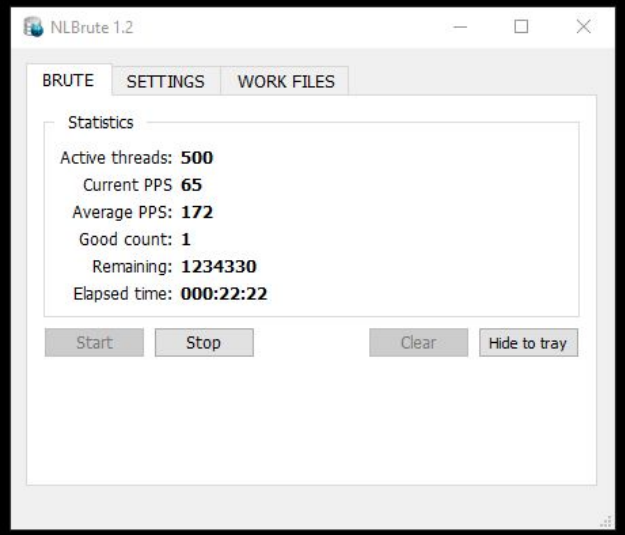
sum(GB)	timestamp
3431.4820615391880000000	11/22/2019 00:00:00
3957.5689774698503000000	11/23/2019 00:00:00
1982.5828443384550000000	11/24/2019 00:00:00

Pools	Indexers	Volume used today
auto_generated_pool_enterprise		1,691,500 MB / 61,440 MB
	hdf-cptc-03.rit.edu	852,509 MB (1,387.547%)
	hdf-cptc-04.rit.edu	838,991 MB (1,365.545%)

Quotent Quotables

- “What’s a modem?”
- “How do you plug this ATM into the ethernet?”
-


asx7j4fYCHxmFZ4D5k
YOUR FILES ARE ENCRYPTED
Don't worry,you can return all your files!
If you want to restore them, follow this link: zombietry4o3nzeh.onion/?ticket=asx7j4fYCHxmFZ4D5k_5CA2F773
Use Tor Browser to access this address.
If you have not been answered via the link within 12 hours, write to us by e-mail: recoverysql@protonmail.com
Attention!
Do not rename encrypted files.
Do not try to decrypt your data using third party software, it may cause permanent data loss.
Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.


NLBrute 1.2
BRUTE
SETTINGS
WORK FILES
Statistics
Active threads: 500
Current PPS 65
Average PPS: 172
Good count: 1
Remaining: 1234330
Elapsed time: 000:22:22
Start
Stop
Clear
Hide to tray

6:37 PM
11/20/2019

the Confidentiali

Hi Tom,

We sincerely apologize but during the course of t
inconvenience.

Sincerely,

Hello!
Is the website dinobank.us considered part of the assessment scope? Also, when can we expect our teammate back from the presentation?

Thanks!

To Tom Dickson <tom.dickson@dinobank.us>
Subject **About Some credentials that we were able to grab**
Date Oct 12th

Hi Tom,

We were able to get some employee credentials in the database, any idea what they might be used for? we would like to further asses the risk of this vulnerability.

Regards,

protected.

to me

Mr Dickens

Our organiz
additional i

Sincerely,

nobank.us>
e were able to grab

We were able to get some employee credentials in the database, any idea what they might be used for? we would like to further asses the risk of this vulnerability.

Regards,

To: Tom Dickson <tom.dickson@dinobank.us>

Dear Tom,

We acknowledge your request. Our team would like to have this in writing s
Thanks, Tom.

abase. **If this data is breached, DinoBank could be shut down.**

```
index=* host="northeastern-t2*" OR host="*t2.northeastern.cptc.network" dest_ip="10.0.1.250" | stats count by src_ip
```

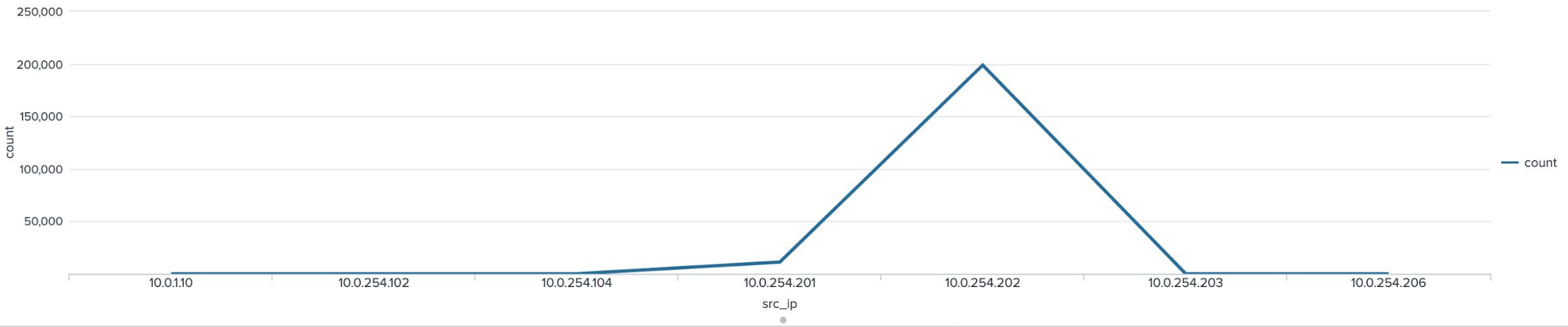
Last 4 hours

✓ 210,086 events (10/12/19 2:20:00.000 PM to 10/12/19 6:20:09.000 PM) No Event Sampling

Job | Verbose Mode

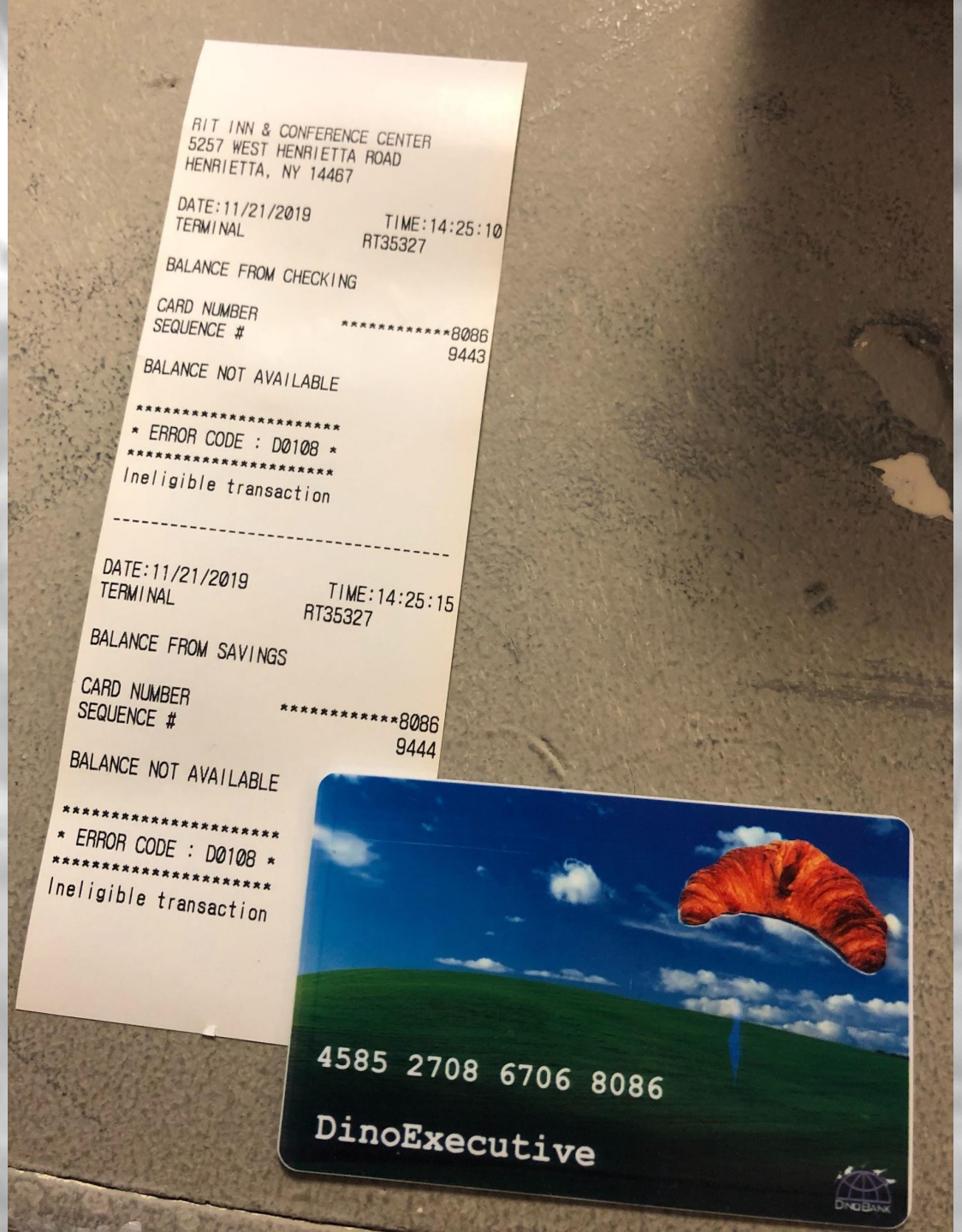
Events (210,086) Patterns Statistics (7) **Visualization**

Line Chart | Format | Trellis



```
**********************
PS C:\Users\Administrator> sudo apt-get install wireshark
**********************
Windows PowerShell transcript start
```

Windows user accounts are also of at least medium strength. We obtained a hash dump and spent around six hours trying to crack them without success. However, we did not have access to powerful hardware or a dinosaur themed wordlist that may have made them much quicker to crack.


RIT INN & CONFERENCE CENTER
5257 WEST HENRIETTA ROAD
HENRIETTA, NY 14467
DATE:11/21/2019 TIME:14:25:10
TERMINAL RT35327
BALANCE FROM CHECKING
CARD NUMBER **********8086
SEQUENCE # 9443
BALANCE NOT AVAILABLE
****
* ERROR CODE : D0108 *
****
Ineligible transaction
DATE:11/21/2019 TIME:14:25:15
TERMINAL RT35327
BALANCE FROM SAVINGS
CARD NUMBER **********8086
SEQUENCE # 9444
BALANCE NOT AVAILABLE
****
* ERROR CODE : D0108 *
****
Ineligible transaction
4585 2708 6706 8086
DinoExecutive
DINOBANK

Cost estimates....

$45 / 6 = $7.50/person

Cost Estimate

Description	Quantity	Cost Per Hour	Subtotal
On-site penetration testing services, consultant fees for team of six (6)	9 hrs	$ 270.00	$ 2,430.00
Report-writing by a team of six (6)	6 hrs	$ 270.00	$ 1,620.00
Presentation by a team of six (6)	1 hr	$ 45.00	$ 45.00

Total: $4,095.00

Activity Name	Frequency	Duration	Count	Cost
Grey box Penetration Test	Once	12 Hours	1	$ 300,000.00

Key Feedback

- Slow down as you speak
- Think about the risks of taking data
- Determine when you ask for permission, know your scope!
- Consider how your client thinks
- Manage your presence when you communicate (slow down!)
- There are tons of distractions, be prepared and have a strategy


One more thing…

The Coin…

What is a coin check?

The Rules

- Keep your coin close
- If you challenge someone, be prepared to buy them a drink
- If you hand someone a coin during a check, it's now theirs
- Don't edit it, change it, or wear it like jewelry
- Feel free to challenge us… at conferences


Actually… two more things

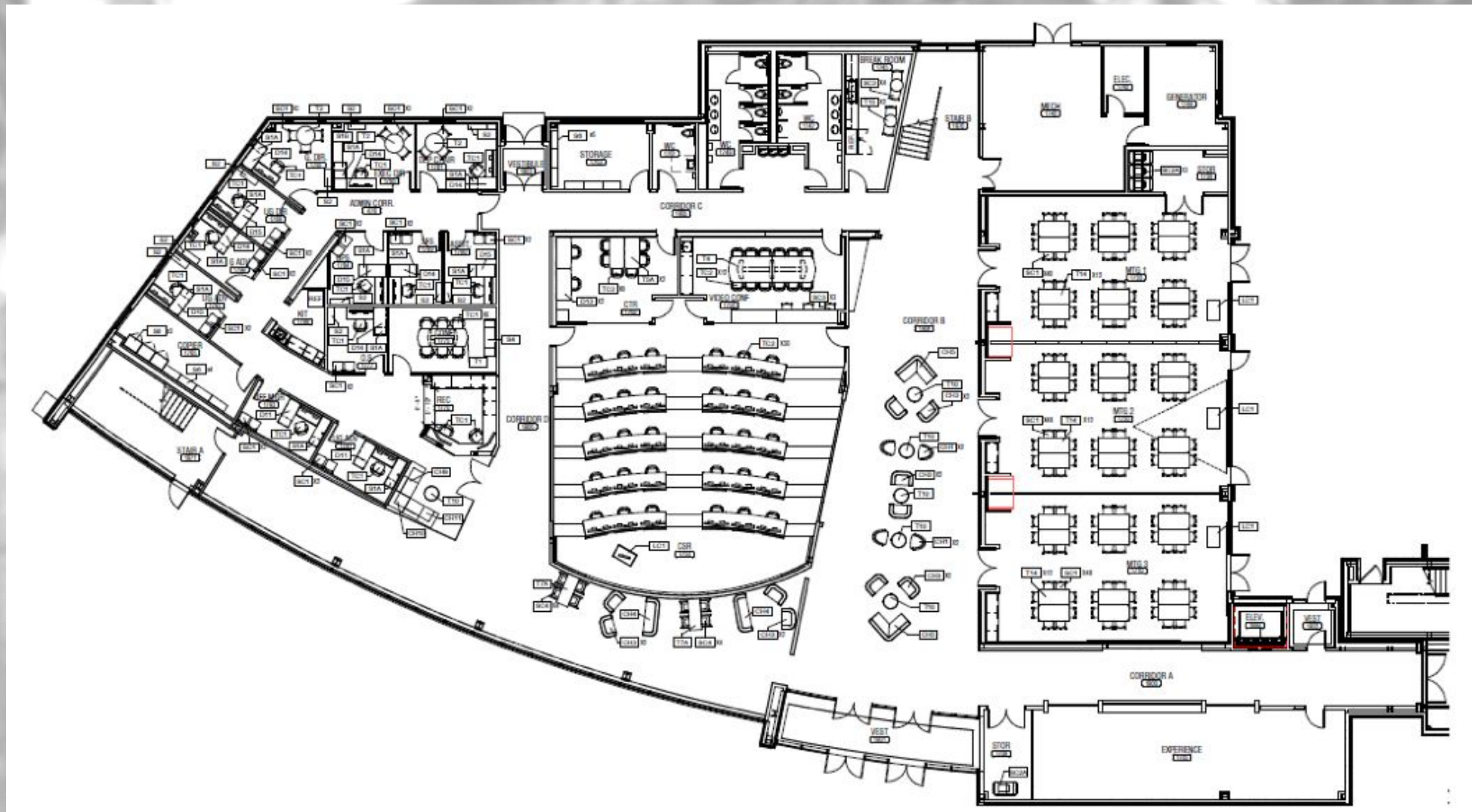
The Future, Is Not Extinct

2020 Logo here

Global Cybersecurity Institute

RIT | Rochester Institute of Te

1st Floor



RIT | Rochester Institute of Te

RIT | Rochester Institute of Te


RIT
Rochester Institute of Te

RIT | Rochester Institute of Te

Multiple Uses

- Cybersecurity degrees
- Workforce development
- Employee certification
- Career change courses
- School and camp courses
- Cybersecurity research
- Event hosting

RIT | Rochester Institute of Te

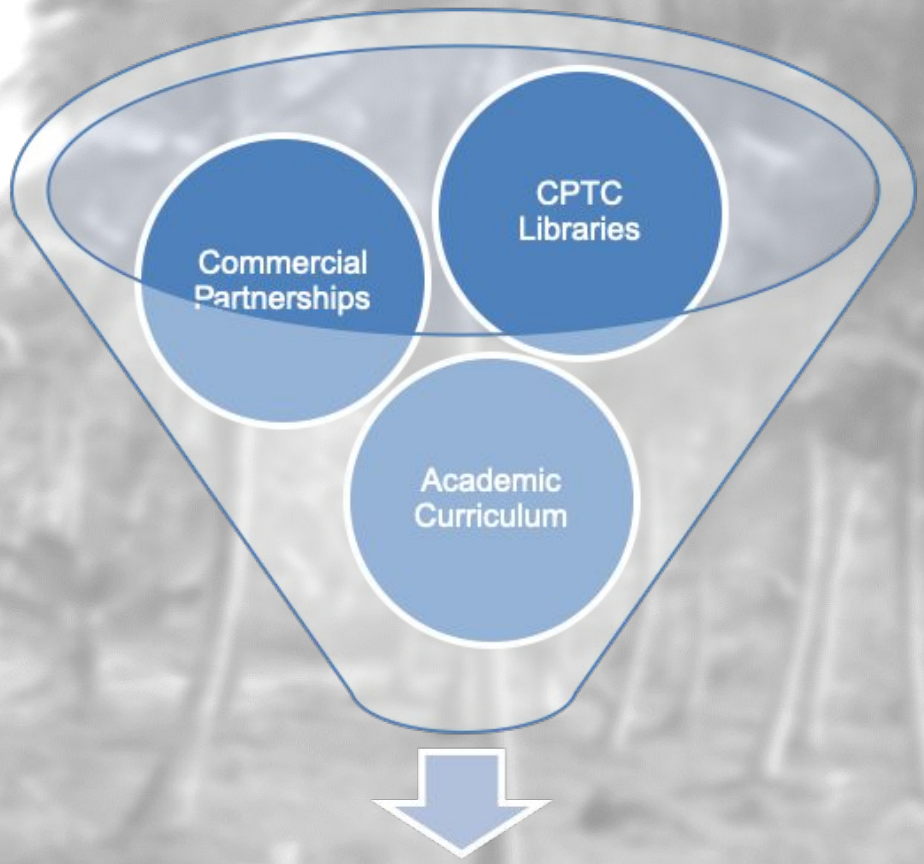
Launch: Fall 2020

>Cloud/On-Prem Hosting

- Green Data Center
- 5,000 simultaneous VMs
- 15,000+ simultaneous OT devices

>Multidisciplinary planning team

- Computing Security / Comp. Sci.
- Magic Spell Studios (Game Design & Prod.)
- Business
- Theatre/Liberal Arts
- Engineering



Cyber Range Scenarios

RIT | Rochester Institute of Te

Five Years

Alex Levinson
Bill Stackpole
Bo Yuan
Bob Kalka
Chris Butler
Daryl Johnson
Colum McGaley
Dave Emlen
Jason Ross
Lucas Morris
Megan Fritts
Tom Kopchak