# Welcome to the Cyber Jungle!

🔑 𝅘𝅥𝅮

00000101

<QUEEN CITY CONFERENCE>

Presented by: **Matt Scheurer**

PDF http://slides.dfirmatt.com

# Welcome to the Cyber Jungle!

🔑 ♪

00000101

<QUEEN CITY CONFERENCE>

Presented by: **Matt Scheurer**

This Slide Deck Has Been Hacked!

-=[ Pwned by the 513 & 859 1337h@x0rZ ]=-

ALL YOUR DATA IS ENCRYPTED!

To unlock your data and recover your files,
send us 42 BTC!

**NEXT**

# So, I gotta ask...

Do you know where you are? You're in the Cyber Jungle, baby...

# Quick showing of hands

On Friday, July 19, 2024

Who here was impacted by the CrowdStrike update, which caused the Windows BSOD issues?

# About Matt Scheurer

I work for a big well-known organization...

As Vice President (VP) of Computer Security and Incident Response (IR). However, I have many years of hands-on technical experience, including Digital Forensics & Incident Response (DFIR).

I am also a Podcast Host for

ThreatReel

https://threatreel.com

Connect / Contact / Follow Matt:

https://www.linkedin.com/in/mattscheurer

https://x.com/c3rkah

# Where I Volunteer...

I am an Official

HACKING
IS NOT A CRIME

Advocate
https://www.hackingisnotacrime.org

WARREN COUNTY
CAREER
CENTER

Advisory Board: Information Technology and Cybersecurity
https://www.mywccc.org/

WOMSA
Empowering Women in Cybersecurity

Women’s Security Alliance (WomSA) Technical Mentor
https://www.womsa.org

# Disclaimer!

Yes, I have a day job. However…

Opinions expressed are based solely on my own independent security research and do not express or reflect the views or opinions of my employer.

# Coaching and Mentorship

Coach S.

I am a big proponent of coaching and mentoring others, which is something I do often!

XXXXX X
OOOOO O
O O

# Matt Scheurer @ QCC 2

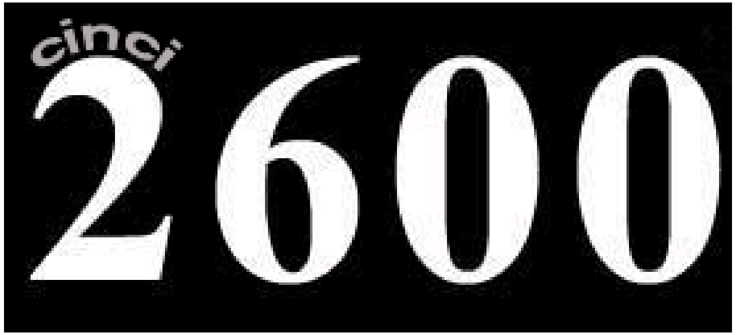
Instructor-Led Lab:
**Wireshark Workshop**
November 15, 2024
11:00 am – 1:00 pm

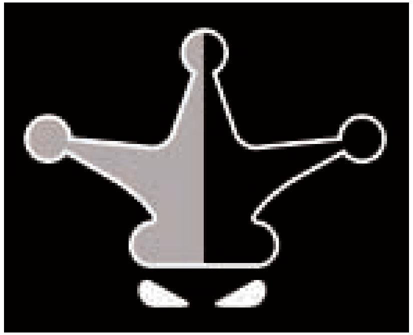
Instructor-Led Lab: **Hands On Password Cracking**
November 16, 2024
10:00 am – 12:00 pm

**Keynote** (Matt Scheurer)
November 16, 2024
2:00 pm – 2:45 pm

**Lies, Telephony, and Hacking History**
November 16, 2024
4:00 pm – 4:45 pm

# A little bit Old School





# My Biggest Challenges

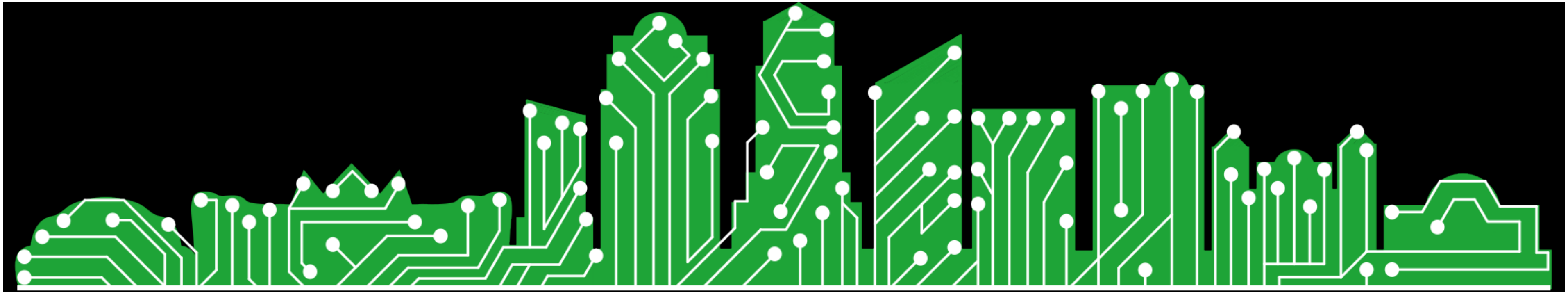
Helping others "Think like an Adversary", &/Or "Truly think like a Security Analyst"

# Mixed Results

*But I keep trying!*

# I’m glad you are all here!

@

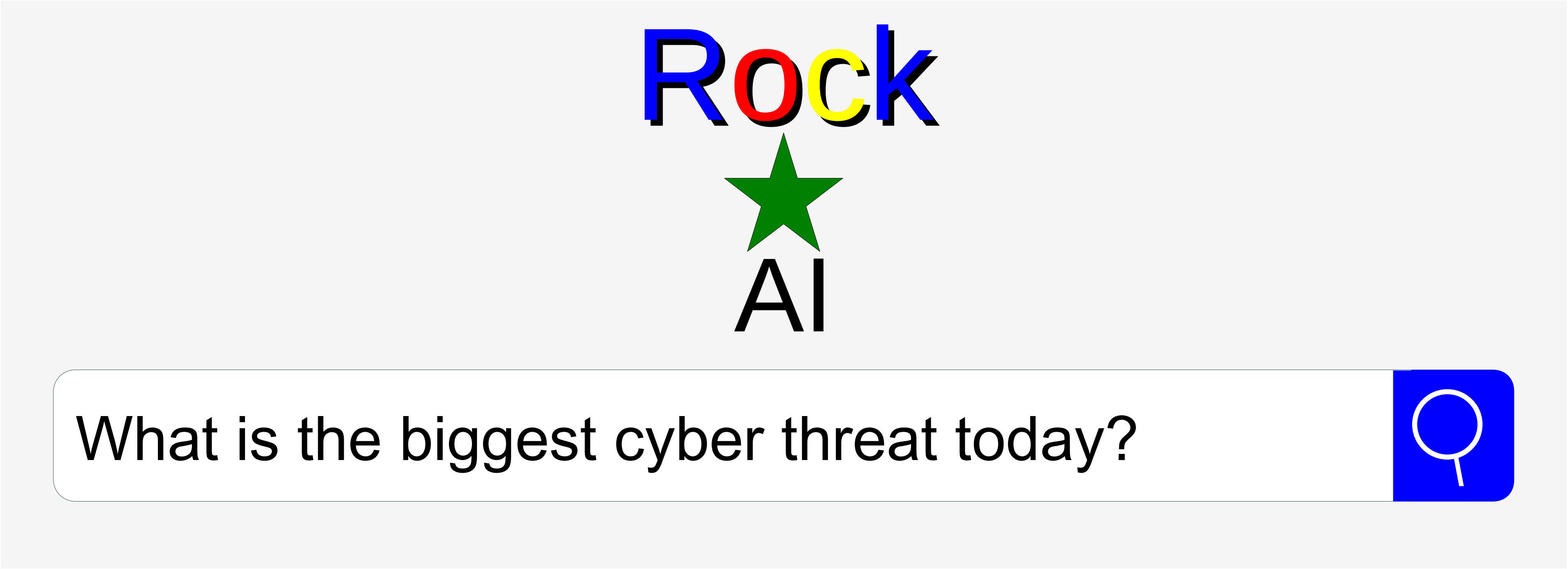


<QUEEN CITY CONFERENCE>

# What is in the Cyber Jungle?

*I needed an infallible expert opinion...*

# So I asked Artificial Intelligence!



What is the biggest cyber threat today?

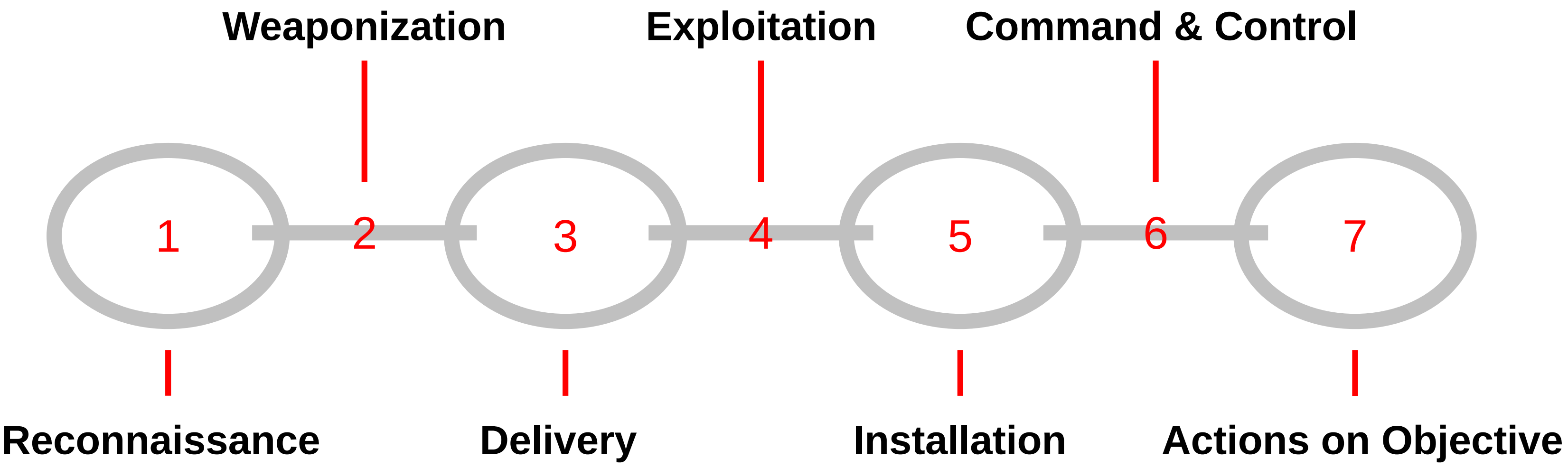
# The Response:

*Ransomware*

# Well,

*let’s think about the “Cyber Kill Chain” for a moment...*

# The Cyber Kill Chain



1 Reconnaissance

2 Weaponization

3 Delivery

4 Exploitation

5 Installation

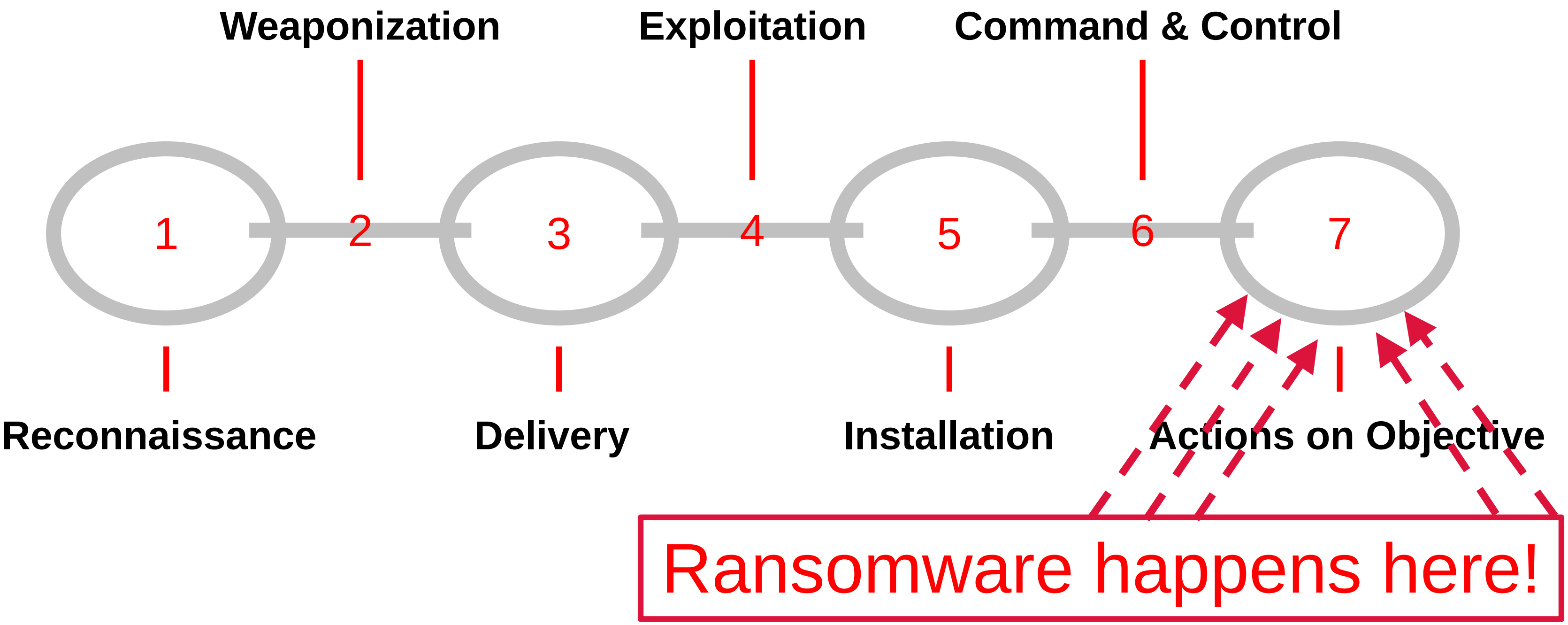
6 Command & Control

7 Actions on Objective

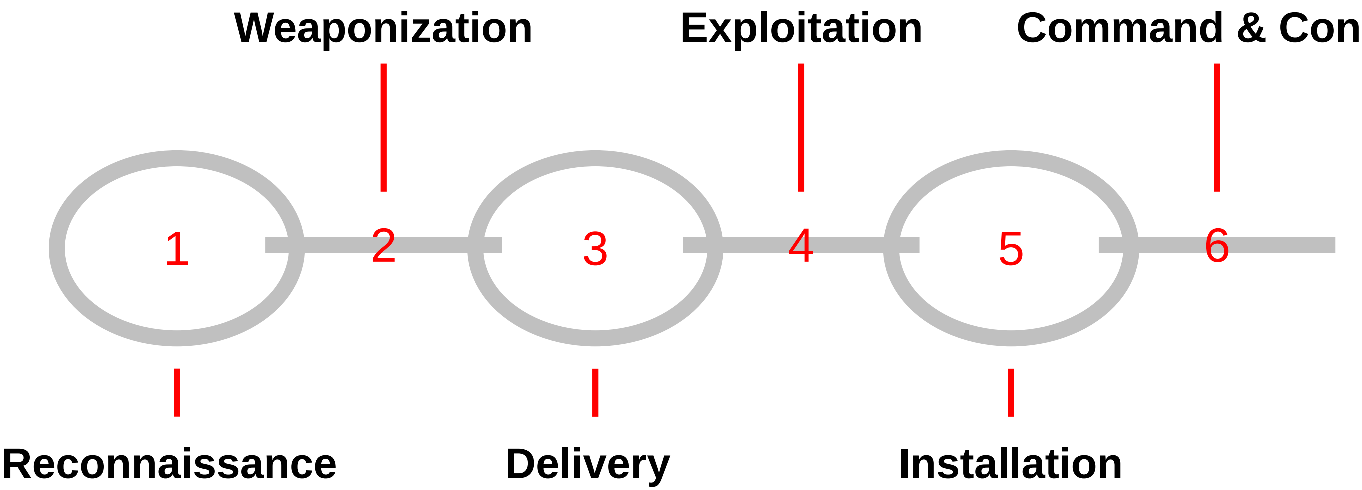
# So,

*the thing is...*

# The Cyber Kill Chain



# Meaning: If we get Ransomware,



We failed to detect and stop the initial compromise at all of these stages first!

# Definitely…

- Plan ahead and execute on those plans
- Incident Response & Digital Forensics
- Legal Counsel and Cyber Insurance
- Lines of Communication
- Public Relations
- Etc.

# By all means...

Have your immutable backups, plus restoration and recovery plans at the ready.

# As my mom would tell you...

An ounce of prevention is worth a pound of cure!

# Sometimes

*Our problems are self-inflicted...*

# A friend recently told me

*it’s okay for everyone to laugh at your pain...*

# That friend

# A SaaD Story to tell

# A SaaD Story to tell

What is “SaaD” you ask?

# A SaaD Story to tell

What is “SaaD” you ask?

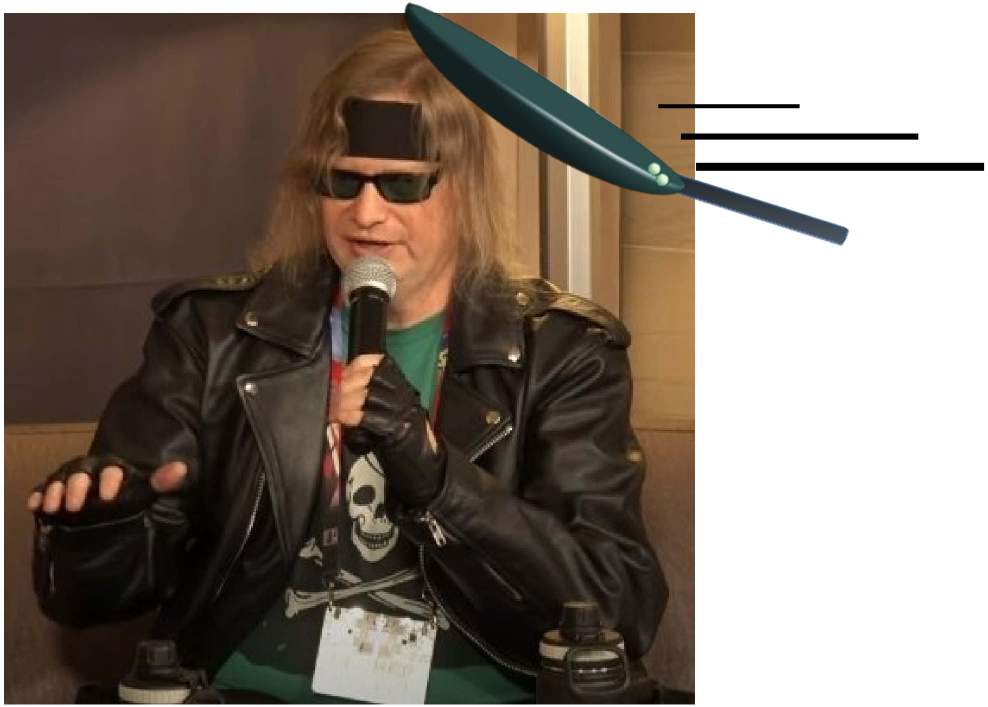
**S**tupidity

**a**s

**a**

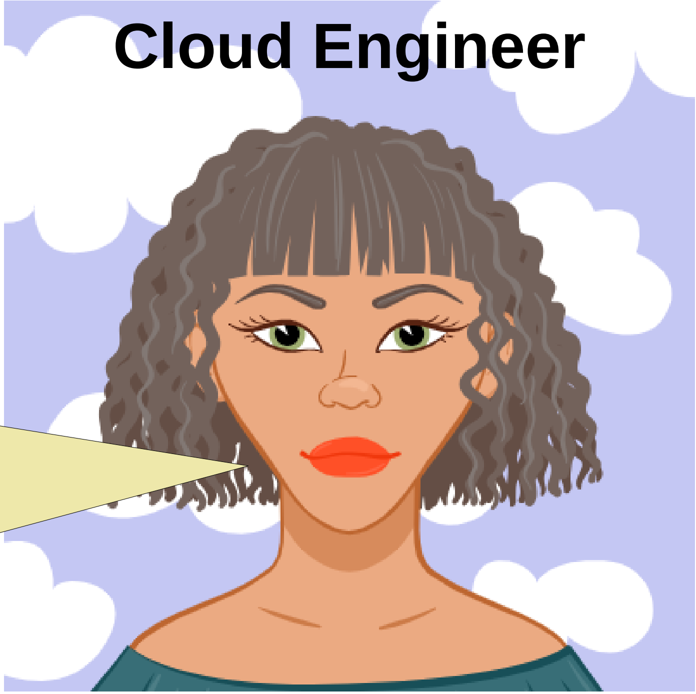
**D**isservice

# SaaD Story: Hit with a frying PAN

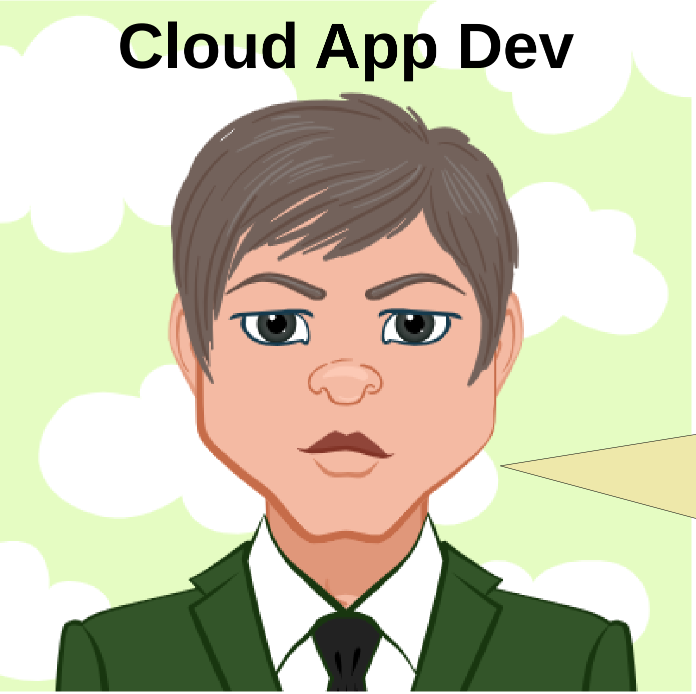


# In the Beginning

Isn't that red warning triangle telling you that this cloud storage shouldn't be publicly readable, concerning?



# False Sense of Confidence



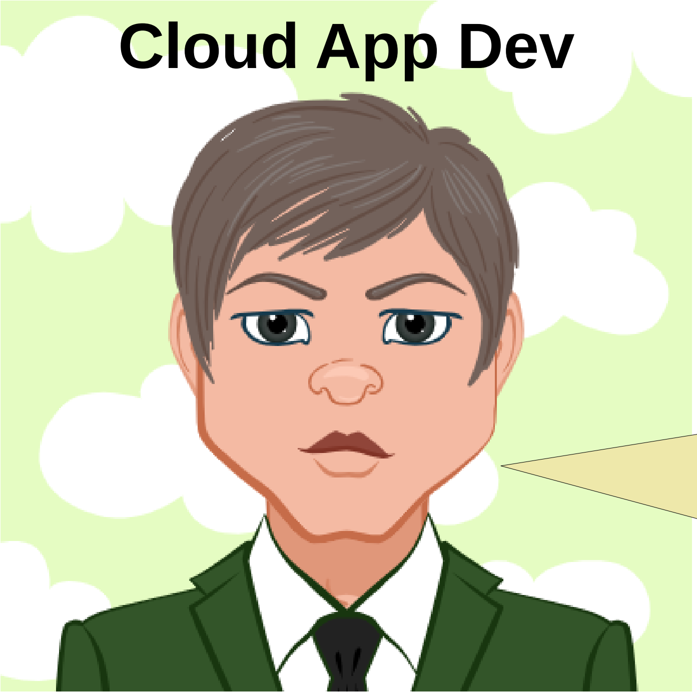
Nah, the cloud application won't permit anything nefarious. Users must login to upload and access data.

# The Notification

Hey, we just got hit with a data extortion email. What's going on here?

DFIR Matt

# False Sense of Security

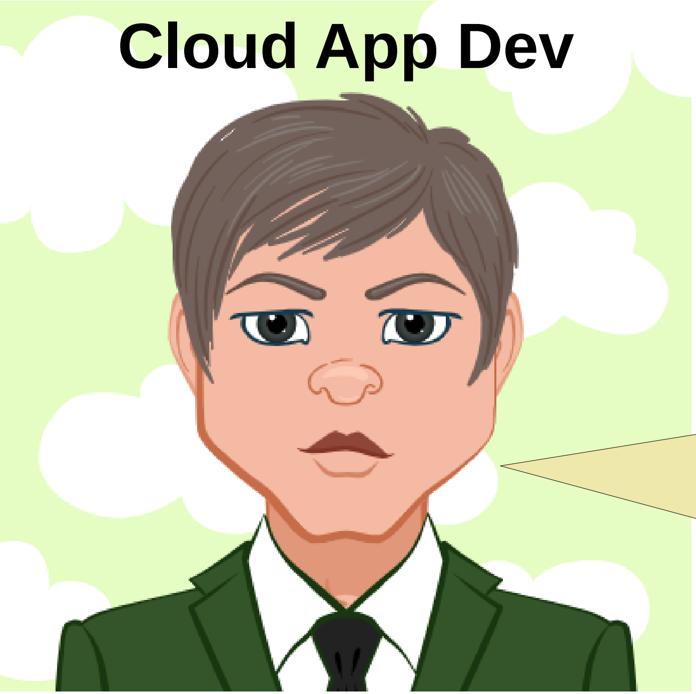


Not to worry, the cloud application wouldn't permit anything nefarious. Users must login to upload & access data.

# This is Nonsense

But it’s configured as *publicly accessible…* Vulnerable to web crawling and web spiders. What is inside the data?

# Clueless about Bad User OpSec



Oh, nothing much…
Just some receipt
image files and
receipt documents.

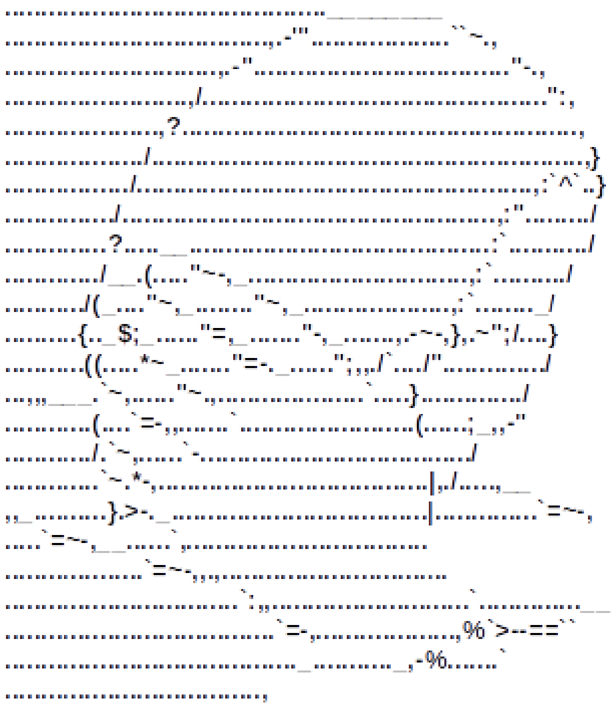
# This just got harder!

Hey, guess what? Reviewing this leaked data, some customers uploaded full credit card details into the system!

# From Bad to Worse

...Now we don't just have data exfiltration, with an extortion attempt, but now also a "Privacy Incident".

# SaaD Story: Advice



- Avoid allowing public access to cloud storage
- Know what details are in your data
- Protect the users from themselves

# QCC Attendees

- Please take advantage of the learning opportunities here
  - Work on learning to think like an adversary
  - Think about the security ramifications of everything

# And,

To help some of you with learning to “think like an attacker”...

# Questions

Who?

What?

When?

Where?

Why?

How?

# Welcome to the Cyber Jungle!

🔑 ♪

00000101

<QUEEN CITY CONFERENCE>

Thank you for attending!

PDF http://slides.dfirmatt.com