Cloud Security Alliance (CSA)

Cleveland Chapter

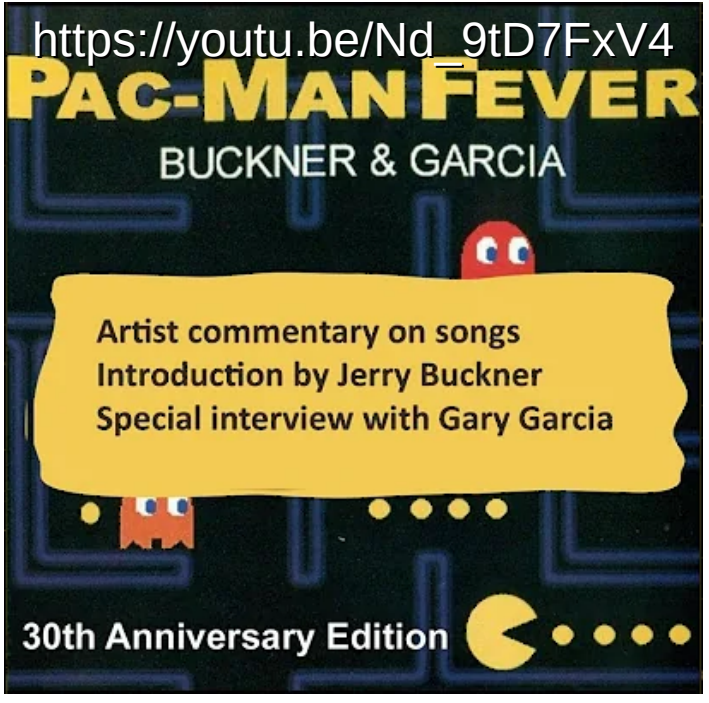
PRESENTS

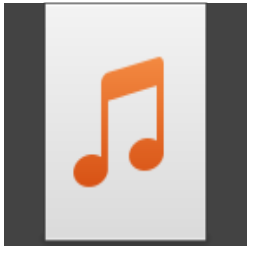
Matt Scheurer, as

THE

DEFENDER

Intro Song: “The Defender”





...Or the 30 second clip’s worth that I can legally stream live (if it works!)

About Me

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://twitter.com/c3rkah

Where I volunteer...

I am an Official

Advocate
https://www.hackingisnotacrime.org

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

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.

Agenda

- Review some major cloud security problems

Agenda

- Review some major cloud security problems
- Cover some cloud-specific security strategies

Agenda

- Review some major cloud security problems
- Cover some cloud-specific security strategies
- Then laugh at my pain...

Agenda

- Review some major cloud security problems
- Cover some cloud-specific security strategies
- Then laugh at my pain...
  - And have a heck of a good time doing so!

Some Cloud Security Issues

- Mostly preventable, but scary!

Some Cloud Security Issues

- Mostly preventable, but scary!
  - Accidental Exposure

Some Cloud Security Issues

- Mostly preventable, but scary!
  - Accidental Exposure
  - Shared Secret leaks

Some Cloud Security Issues

- Mostly preventable, but scary!
  - Accidental Exposure
  - Shared Secret leaks
  - Lack of Visibility (Assets Management)

Some Cloud Security Issues

- Mostly preventable, but scary!
  - Accidental Exposure
  - Shared Secret leaks
  - Lack of Visibility (Assets Management)
  - Shadow & Vulnerable APIs

Some Cloud Security Issues

- Mostly preventable, but scary!
  - Accidental Exposure
  - Shared Secret leaks
  - Lack of Visibility (Assets Management)
  - Shadow & Vulnerable APIs
  - Inadequate Logging

Specific Security Tips

AWS Security Components

- GuardDuty
  - Monitoring, detection, and alerting
- CloudTrail
  - Activity and event logging
- CloudWatch
  - Performance monitoring & analysis

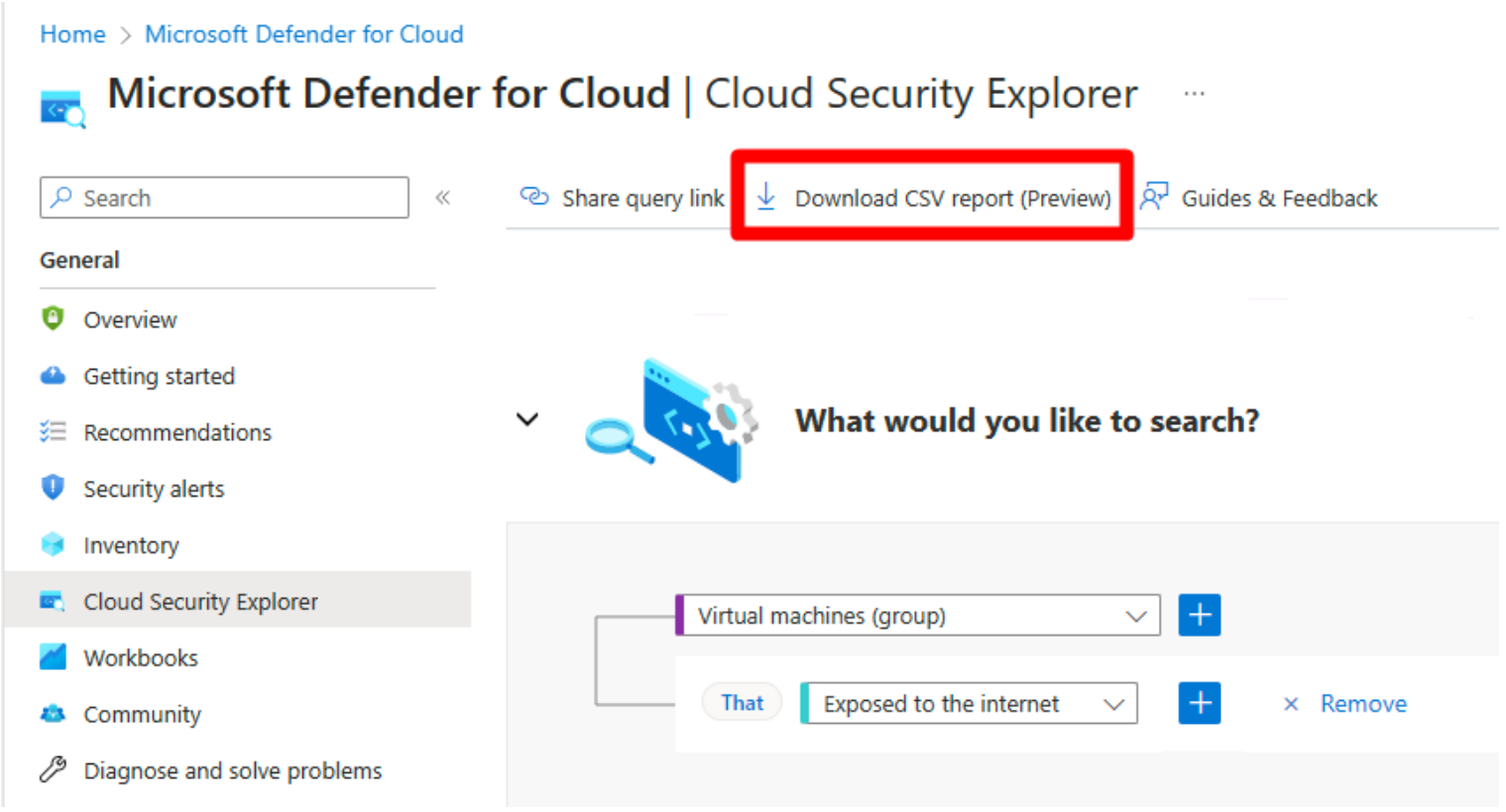
AWS Security Training

- fl**AWS**
  - https://flaws.cloud
- fl**AWS**2
  - https://flaws2.cloud

Azure Attack Surface Reduction

- Cloud Security Explorer
  - Build cool queries
  - Hunt for, and find bad stuff before the threat actors do!

Cloud Security Explorer



Azure Security Training

- Kusto Detective Agency
  - https://detective.kusto.io/
- SC-200 Training
- Microsoft Security Academy
  - Links to “Ninja” Trainings

GCP Attack Surface Reduction

- Security Command Center

state=”ACTIVE” AND NOT mute=”MUTED” AND category=”PUBLIC_IP_ADDRESS”

GCP, Automated IR

- **CAFIR**
  - By Matt Coons (a.k.a. ArborBytes
  - Cloud Automated Forensics & Incident Response
  - https://github.com/ArborBytes/CAFIR

Introducing: DaaD

Introducing: DaaD

What is “DaaD” you ask?

Introducing: DaaD

What is “DaaD” you ask?

DaaD: Story #1

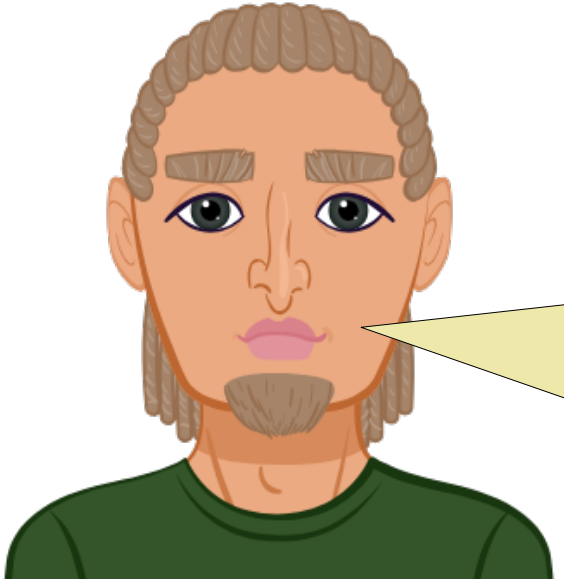
Of course, we did. (NOT!)

DaaD: Story #1

Hey <app owner>, I just got a pen test alert that they found and were able to sign into the cloud-hosted web <app> portal. Did you ever change the default admin account?

DaaD: Story #1

Application Owner



Definitely! We always change default account usernames, where possible, and change the default passwords, each time we deploy an application.

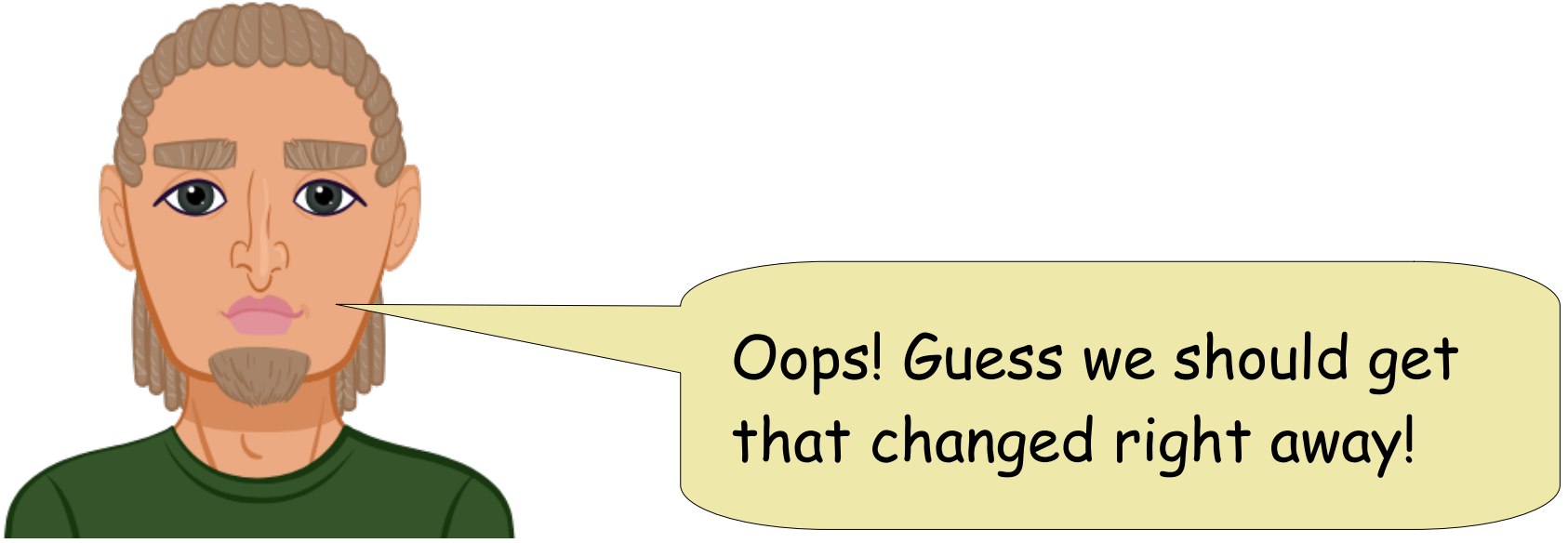
DaaD: Story #1

Minutes later…

Hey, I just tested myself, and got right in using the default creds. All the data, accounts, configs, settings, ability to add new accounts to the platform…

DaaD: Story #1

Application Owner



DaaD: Story #1

Yes, that's an immediate need! Now we need to look and make sure there aren't unauthorized accounts in here. Analyze the level of data exposure. And look for unauthorized access.

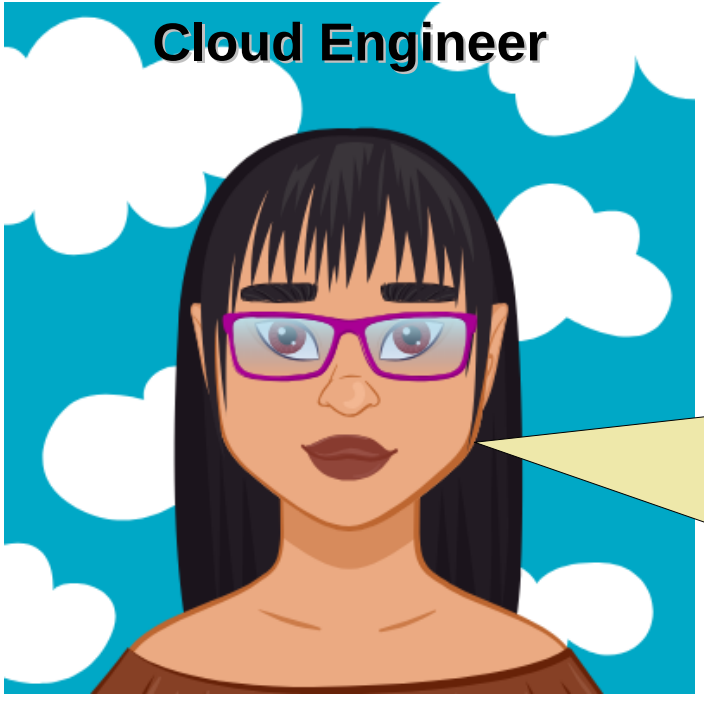
DaaD Story #1: Advice

- Always change all your application default credentials
- Also, actively test for default credentials

DaaD: Story #2

Is that a data lake or a data leak?

DaaD: Story #2



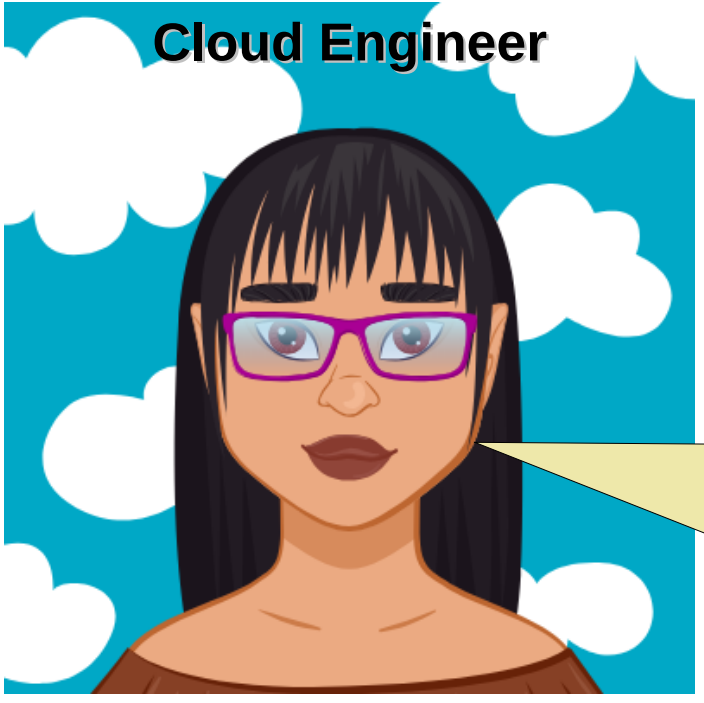
Hey <app owner>, before we migrate this application over to our primary cloud environment, does the database contain any PII data that we need to be concerned about?

DaaD: Story #2

Application Owner

No, our database doesn't contain any PII or any other sensitive data that we need to be concerned about.

DaaD: Story #2



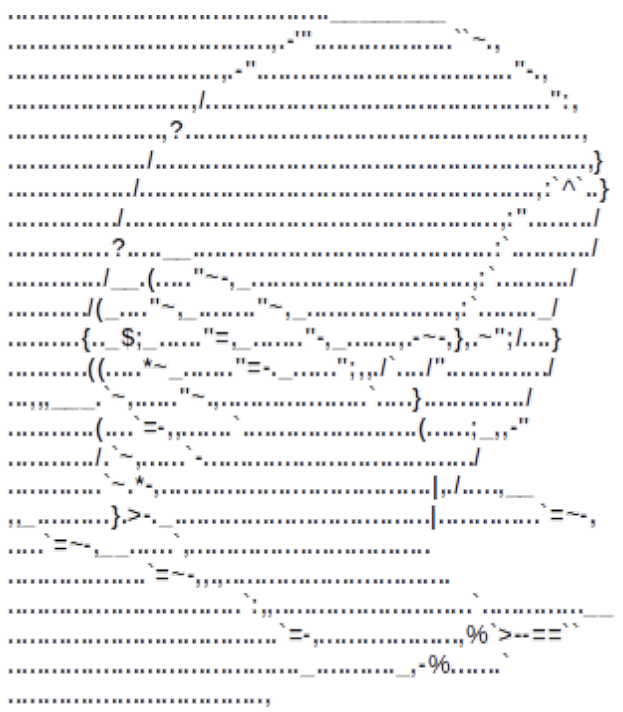
A couple of Months later…

Hey <incident response> our data classification scan found the database from this <app>, which was just migrated to the cloud, and contains PII data…

DaaD: Story #2

Well, my day just got busier… We'll get it shut it down now! Then analyze the level of data exposure. And look for any indicators of unauthorized access or data leakage right away!

DaaD Story #2: Advice



- Data governance is very important
- Know what is in your data, before migrating it to the cloud!

DaaD: Story #3

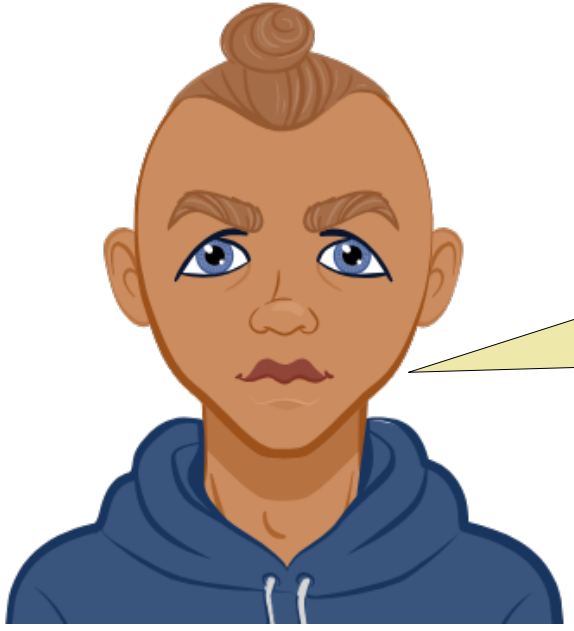
Must be a bad connection.

DaaD: Story #3

Hey <dev lead>, we just got a security alert that one of our cloud hosts is communicating with known <hostile country> crypto-miner IP addresses!

DaaD: Story #3

Dev Team Lead



Not to worry, that is our dev/test environment. Those resources don't have any access to the Internet.

DaaD: Story #3

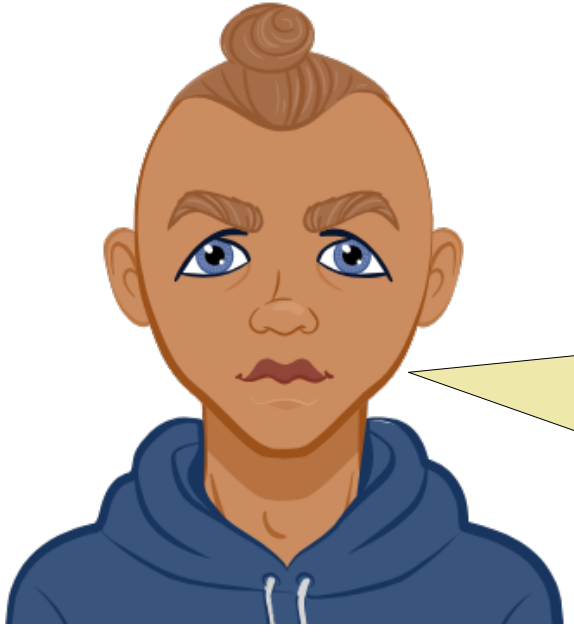
That answer just doesn't make any sense to me. If that is true, then how in the World could this be talking to any known-bad crypto-miner IP addresses?

DaaD: Story #3

Well, the container logs aren't available in the SIEM for some reason. Can we please get the native container logs to investigate this further?

DaaD: Story #3

Dev Team Lead



Unfortunately, no. The logs are all gone. The application has a memory leak problem. So until we fix that, we temporarily purge and recreate those containers every day as a workaround.

DaaD: Story #3

You have got to be kidding me! That is so horrible on so many different levels!

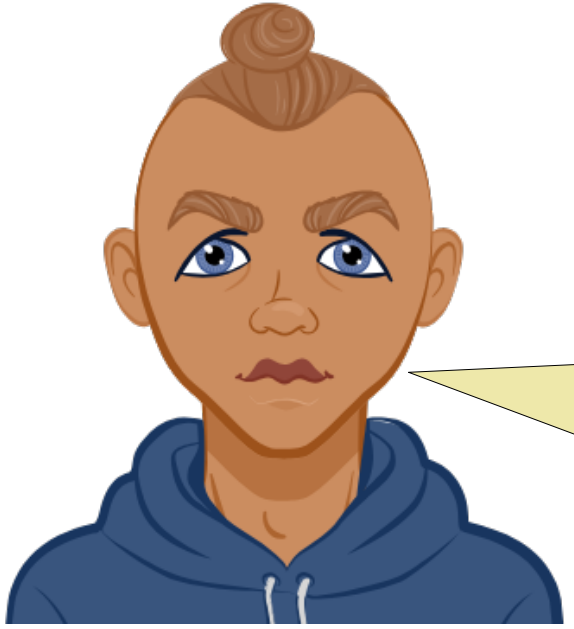
DaaD: Story #3

The following Day…

Hey <dev lead>, that same alert is firing again. We need to investigate this right now!

DaaD: Story #3

Dev Team Lead

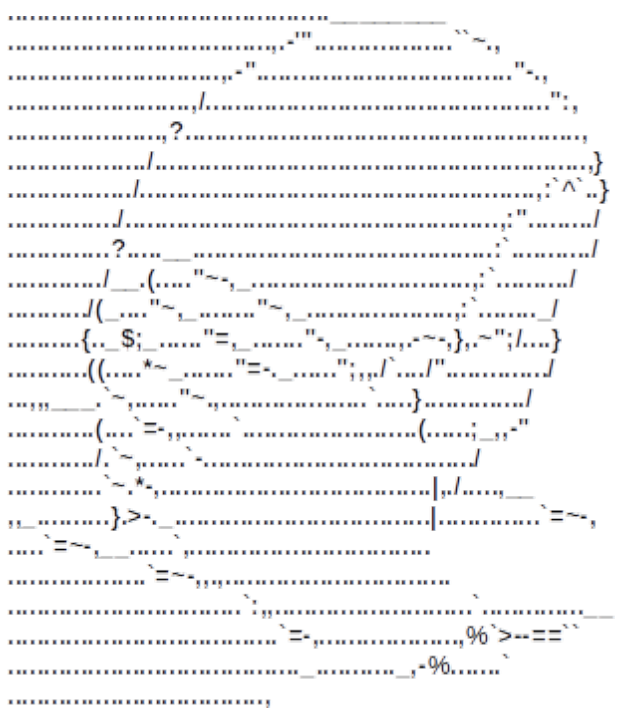


Oh wait. Looks like those containers are sitting behind our load balancer after all! We had no idea, but we can get you the logs right away now.

DaaD: Story #3

You have got to be kidding me! That is so horrible on so many different levels!

DaaD Story #3: Advice



- Retain your log files!
- Understand your environment
  - Even if it’s “just” a dev/test environment

DaaD: Story #4

Sorry (not sorry) to interrupt your vacation...

DaaD: Story #4

Hey <dev manager>, we just got a pen tester finding of RDP listening on a cloud host. The resource owner is currently offline. We need to get this disabled ASAP!

DaaD: Story #4

Dev Manager

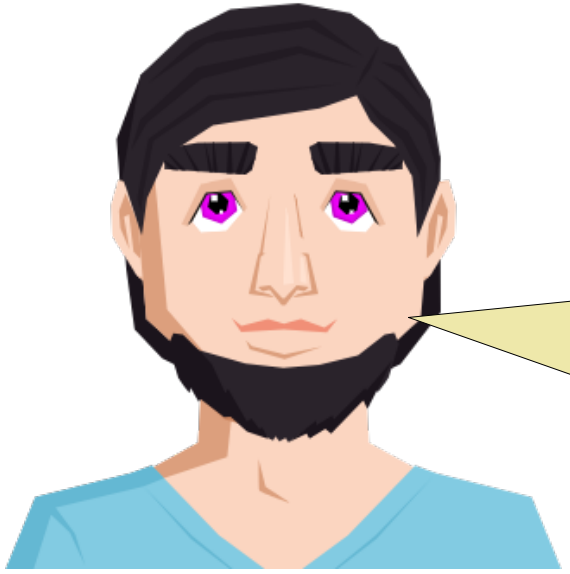
Understood! That developer is currently out on vacation, but I'll reach out to them and have them to join the ongoing investigation call right away.

DaaD: Story #4

Hey <dev>, thank you for joining our phone bridge. We have a host actively allowing RDP access, which is a security risk. We need to get this disabled right away!

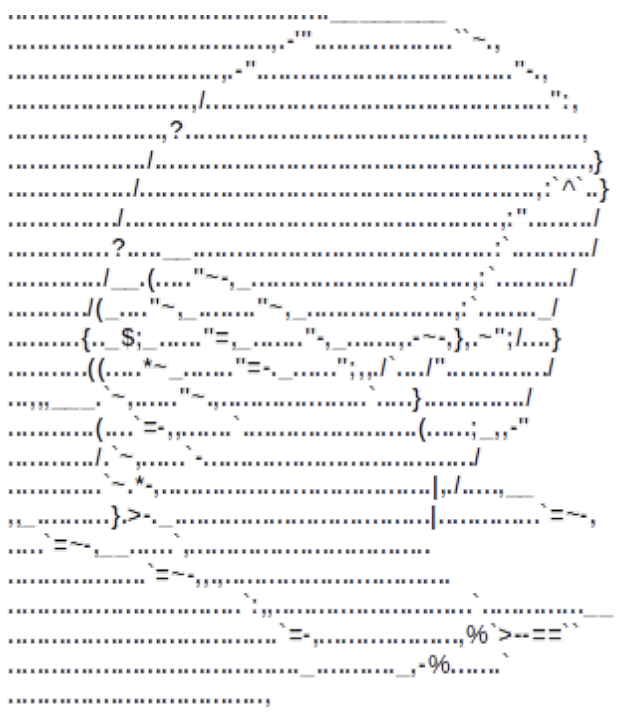
DaaD: Story #4

Developer



Uh, yeah. Sorry about that. I was having VPN problems, and so I just created a temporary jump host to get into to the environment, while I was out on vacation this week.

DaaD Story #4: Advice

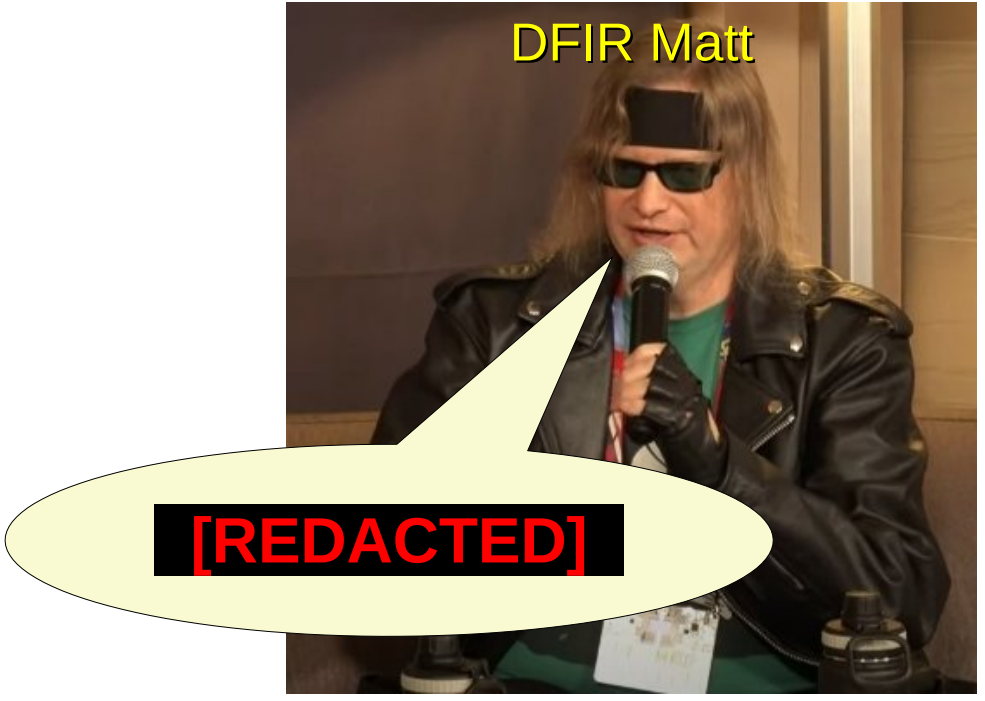


- Don’t circumvent security for convenience
  - Temporary solutions are easily forgotten!
  - No <u>good</u> excuse for <u>bad</u> OpSec!

DaaD: Story #5

Heavy metal, with a large composition of Irony!

DaaD Story #5: (*Sorry!*)



Instead, let's talk about this...

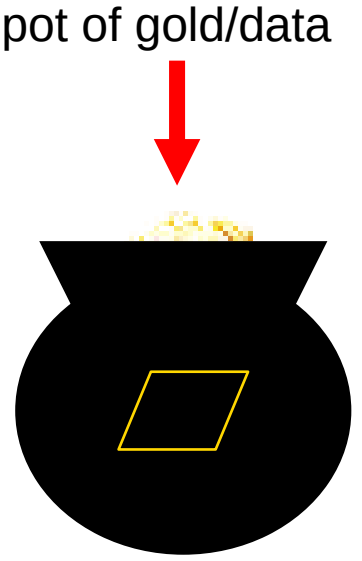
Trending API Risks

- **Accidentally/Publicly exposed APIs**
  - Allows for direct API access
  - Circumvents front-end web & web app security
- **Shadow APIs**
  - Deployed outside of standards and controls

My new slide from "**Hacking Web APIs**"
Cincinnati OWASP, 05/08/2024 meeting

Hypothetical Scenario

- Lets say you have a pot of gold that you want to protect
  - Or a pot of “**data**” if you prefer...

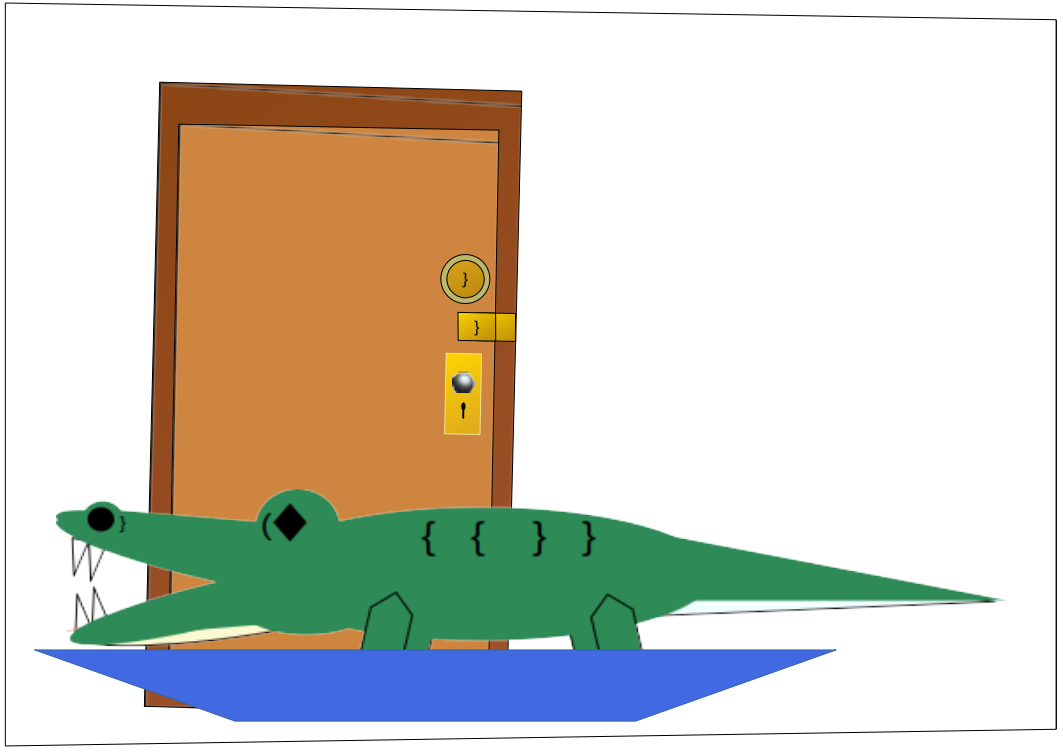


Perimeter Security

Post Orders

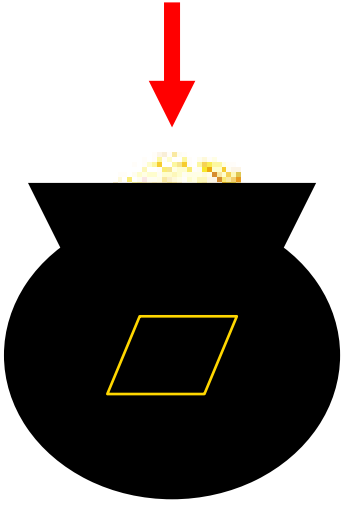
Guard's **only** duty is never allowing any unauthorized person(s) access through the door!

Interior Security

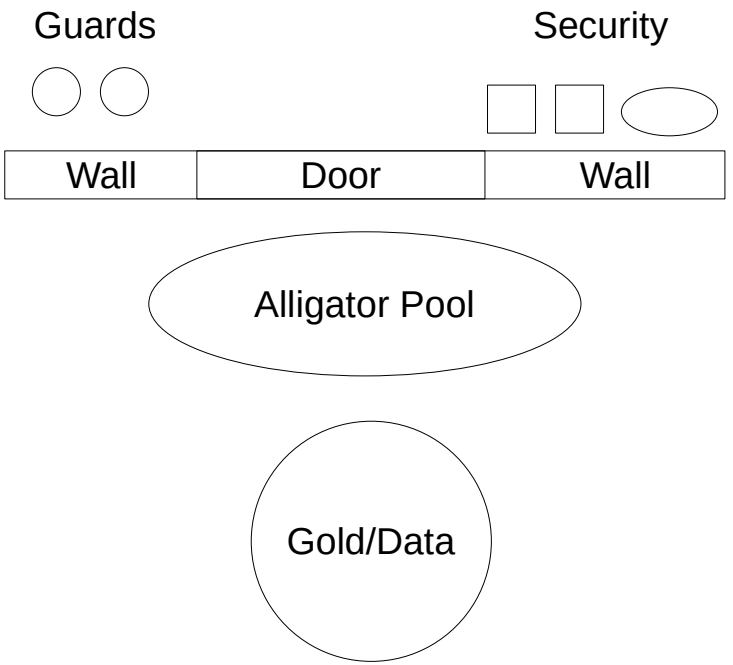


Behind the alligator…

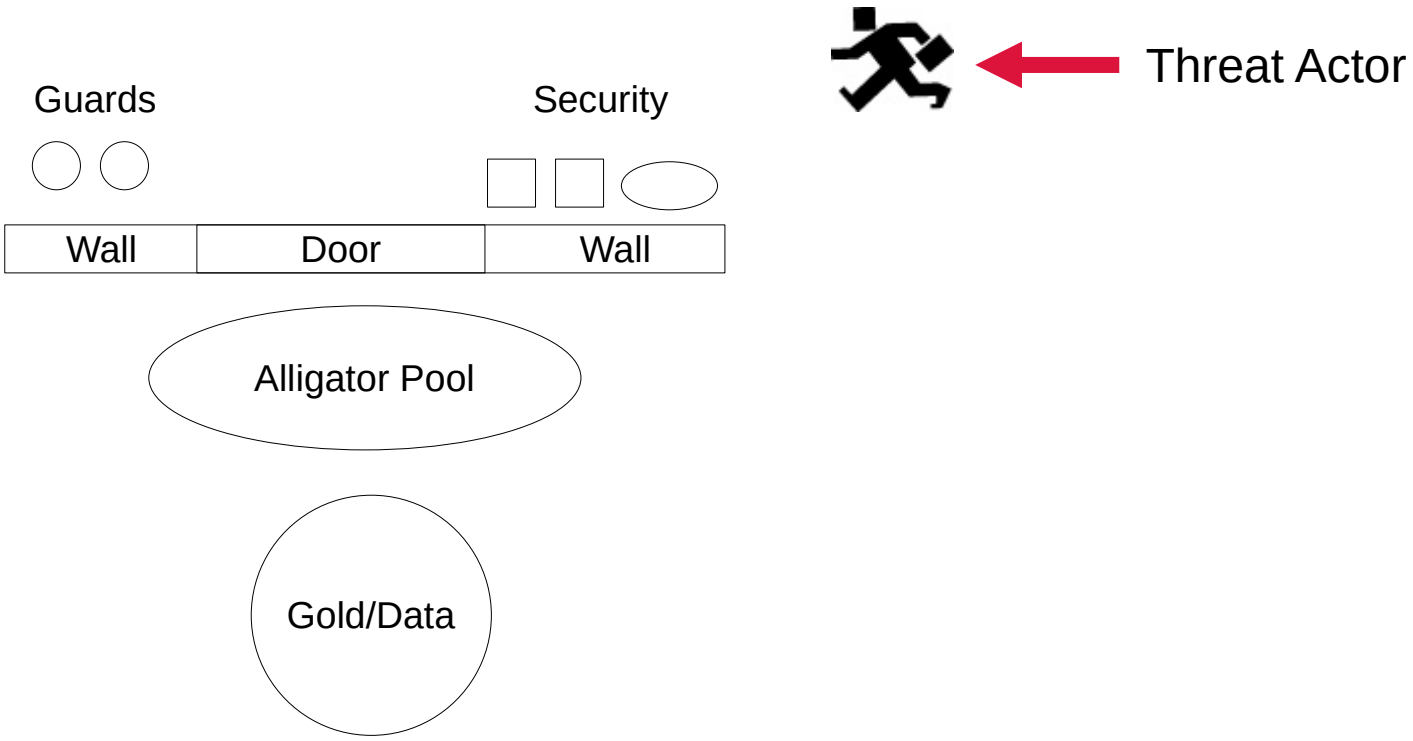
pot of gold/data



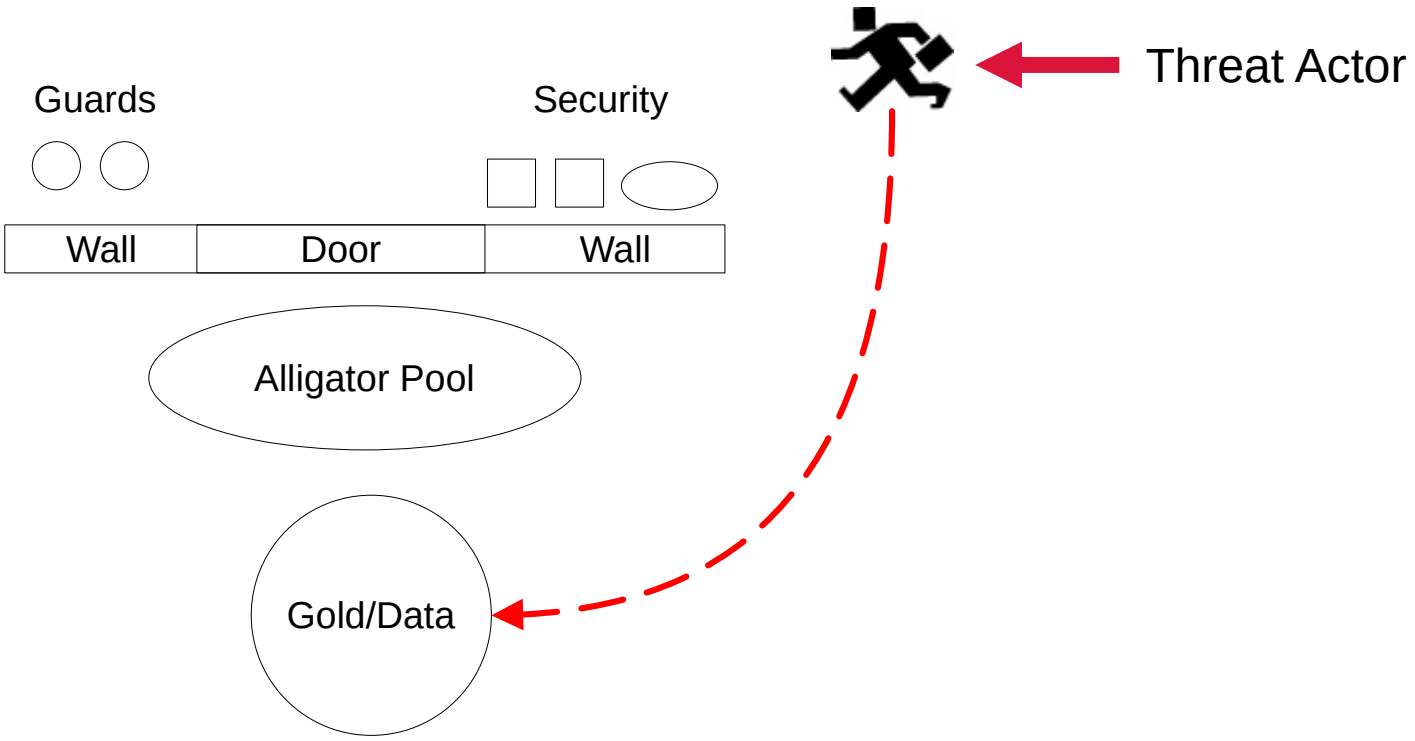
The Floor Plan



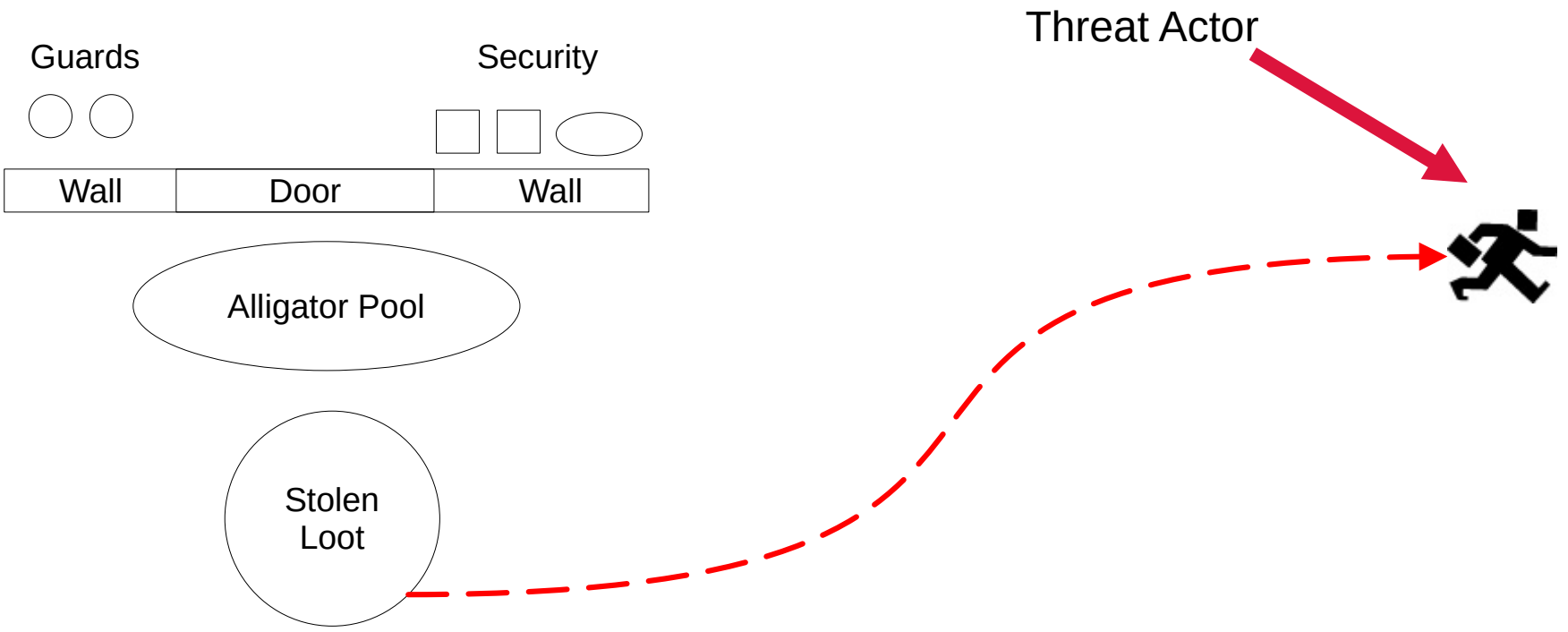
The (Data) Breach



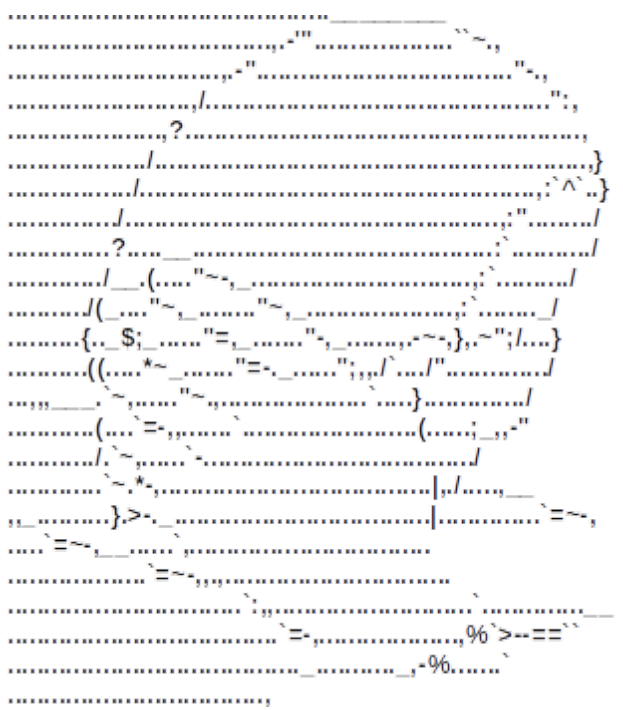
The (Data) Breach



Action on Objectives

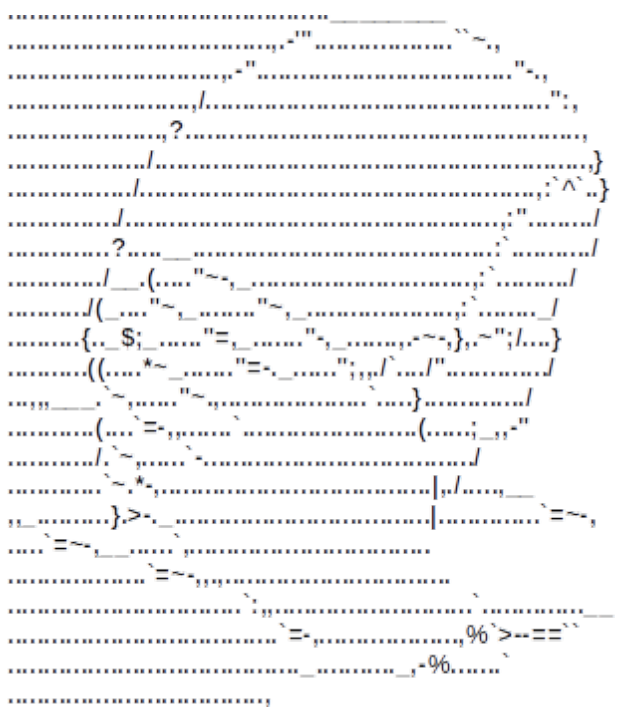


Parting Advice



- Listen to that dude, Matt…

Parting Advice



- Listen to that dude, Matt…
  - He knows what he’s talking about!

Questions

Who?

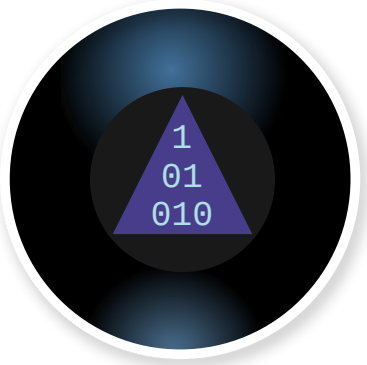
What?

When?

Where?

Why?

How?



Thank you for attending!

Cleveland CSA

PRESENTS

Matt Scheurer, as

THE

DEFENDER