0
0
0
0
0
1
1

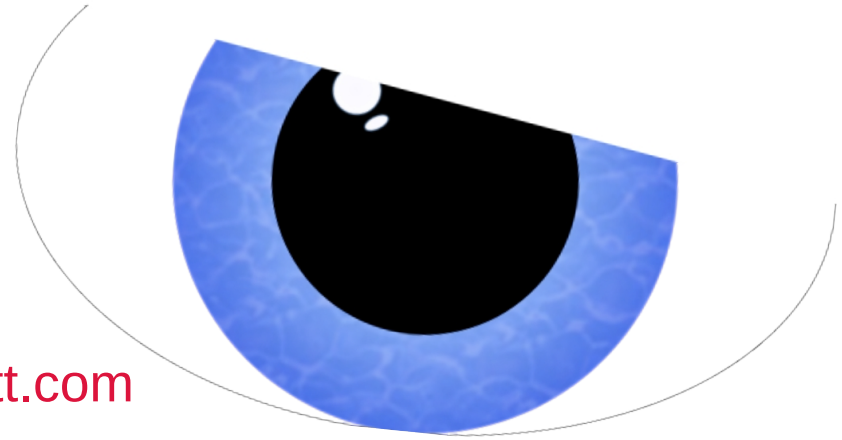
0x3

city of CINCINNATI

11/08/2025

★★★★★

PDF http://slides.dfirmatt.com



Eye of the Responder

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://x.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!

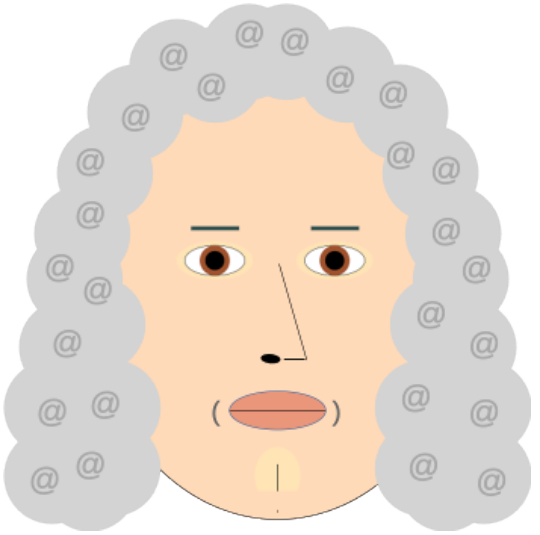
Yes, I have a day job. However…

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

Keynote Perspectives

Keynote Inspiration

- 3rd law of motion
  - For every action, there is an equal and opposite reaction



Sir Isaac Newton

Keynote Theme

For every new thing added into our technology stack, does the attack surface increase?

My Profession

Digital Forensic & Incident Response

I <3 Purple Teaming!

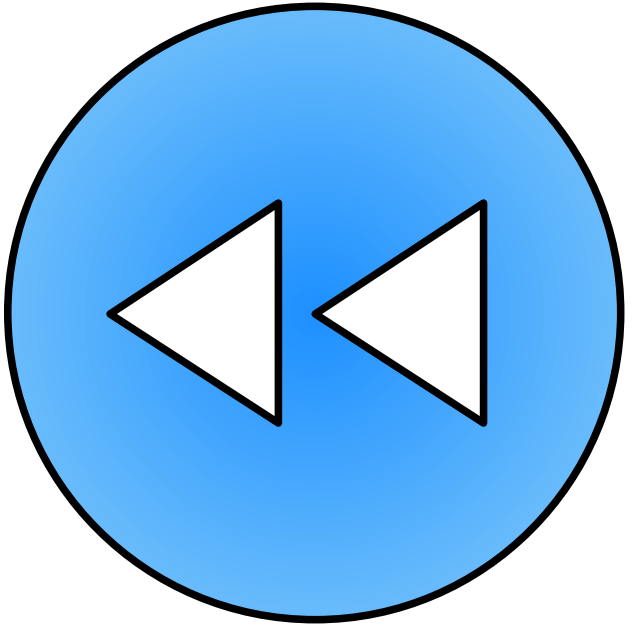
I do Incident Response

ACTION!!!

Why is that?


Attack!
Attack!
Attack!
Attack!
Anything on the Internet
Attack!
Attack!
Attack!
Attack!

Quick DFIR Rewind



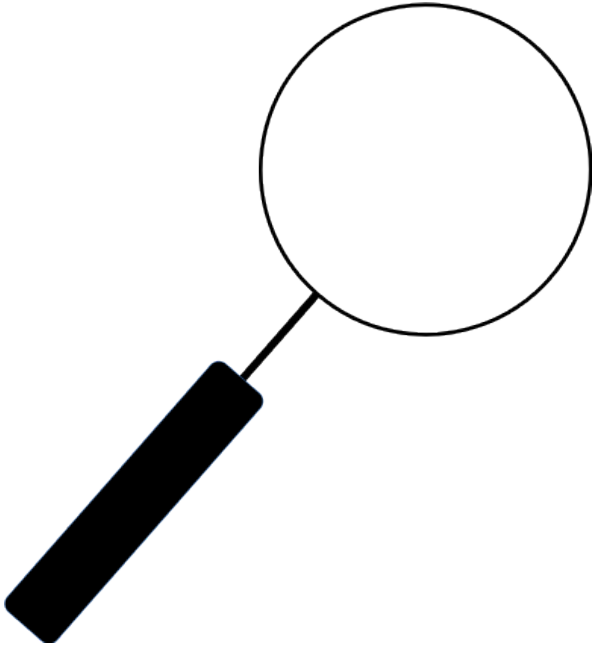
Role of Incident Response

1) Who?
2) What?
3) When?
4) Where?
5) Why?
6) How?

Investigations

Initiated through

- Automated Alerts
- Reports or requests



Data Breach (Top Techniques)

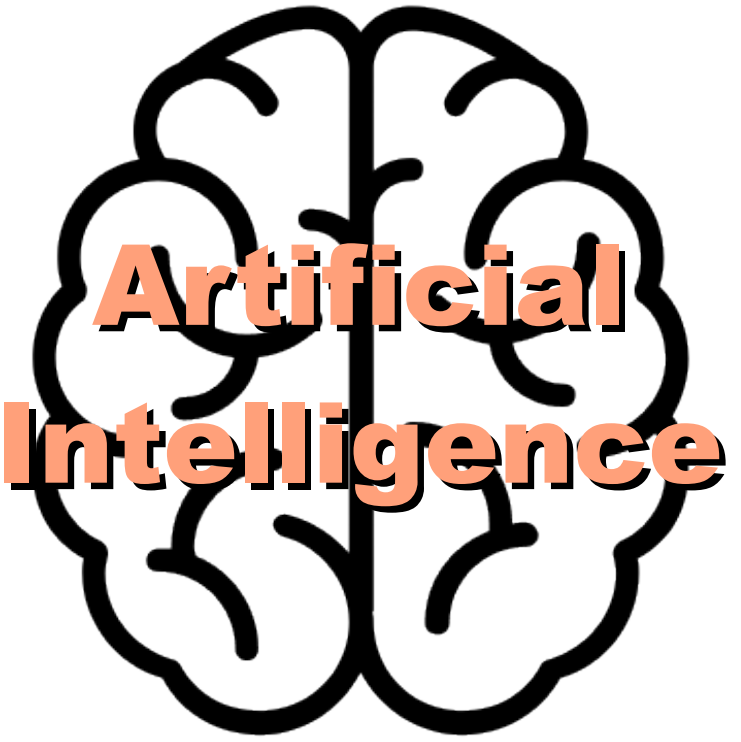
1. Ransomware	6. Defense Evasion
2. Stolen Credentials	7. Network Scanning
3. Exploit Vulnerability	8. Exploit Misconfiguration
4. Phishing	9. Data Leakage
5. Backdoor / C2	10. Disable Controls

** Source = 2025 Verizon DBIR*

Obligatory AI Content

Once Upon a Time...

“The New Hotness”

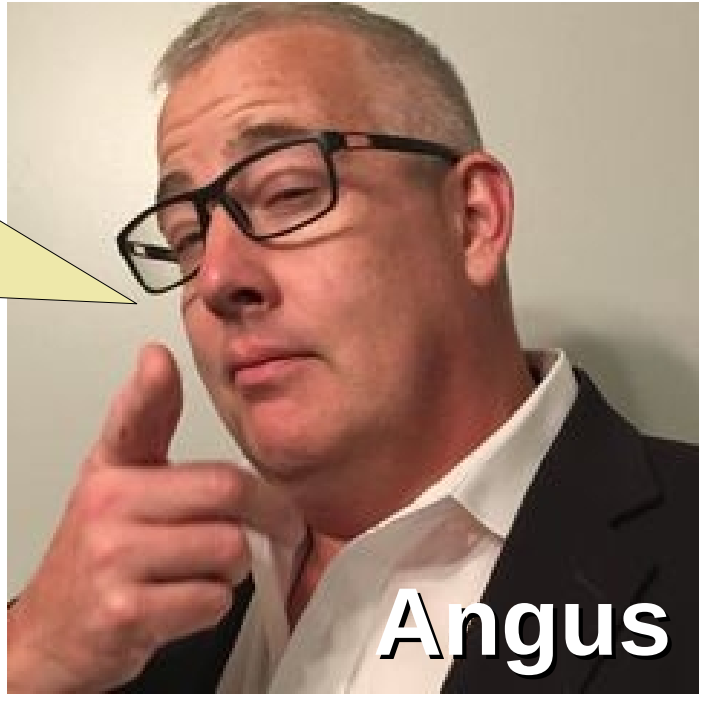


In the Beginning

Now that we've rolled this out to nearly everyone in the enterprise, we should consult with a well-researched industry expert on AI.

Consulting Expert

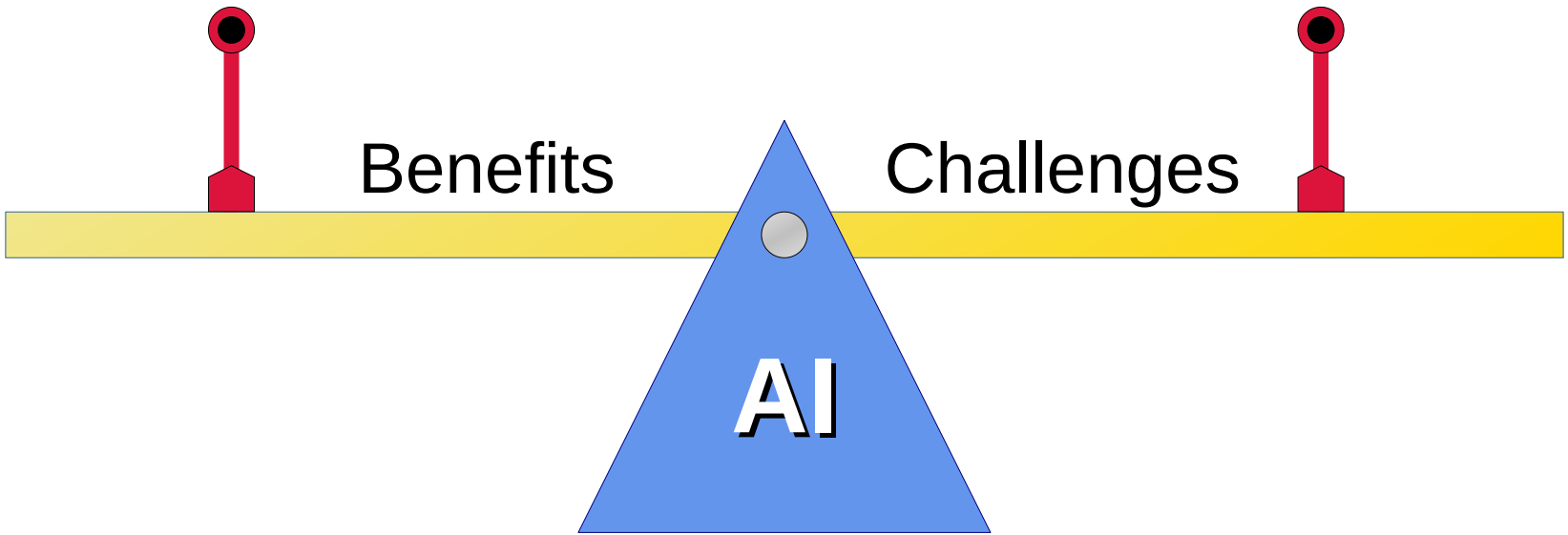
"Don't turn on [AI platform] for everybody at once."



Everyone on the call...

Oops,
Too Late!!!

Balancing Act



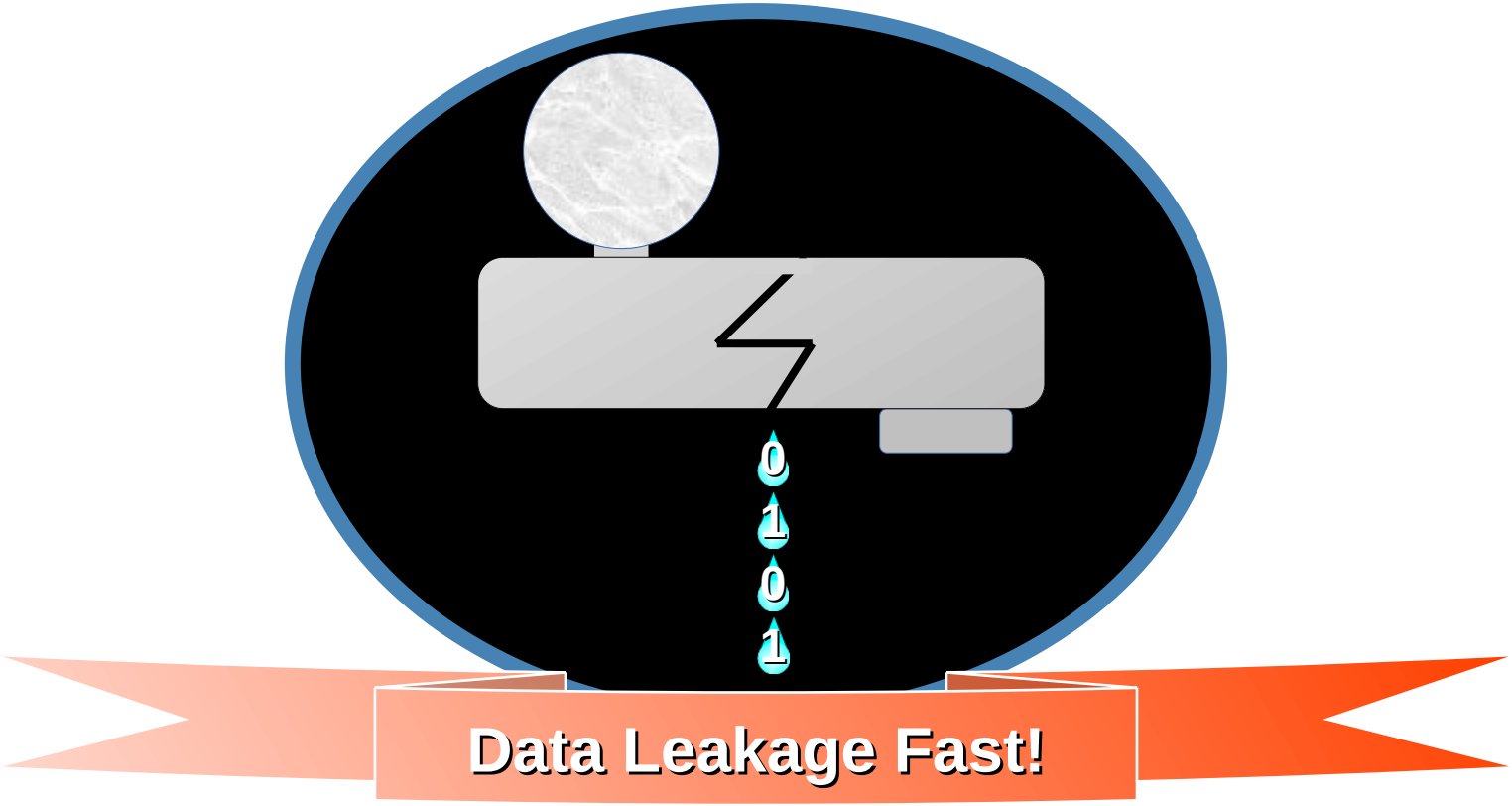
AI is fantastic, but

Unexpected Consequences...

Enterprise AI Observations

AI knows everything about everyone and everything in your environment, if you're not careful!

AI knows your data



AI also knows, “You”!

Emails
Chats
Direct Messages
Meetings
Prompt History

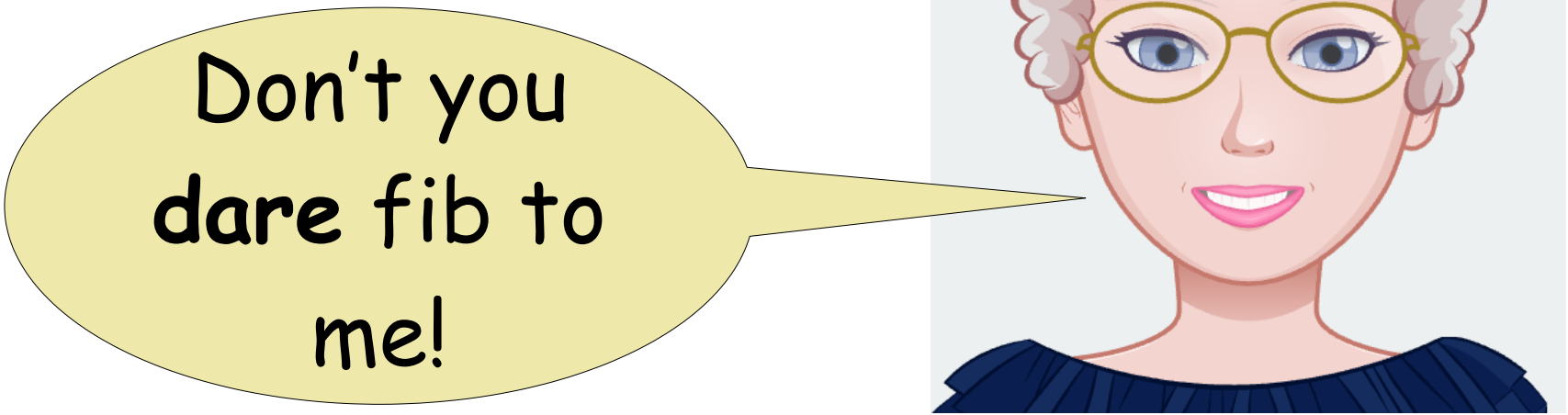
What's worse

- It'll just make stuff up
  - Including: About you!

I have it on good authority that Matt said [thing] on [date] at [time] with [person/group]...

If I told my mother

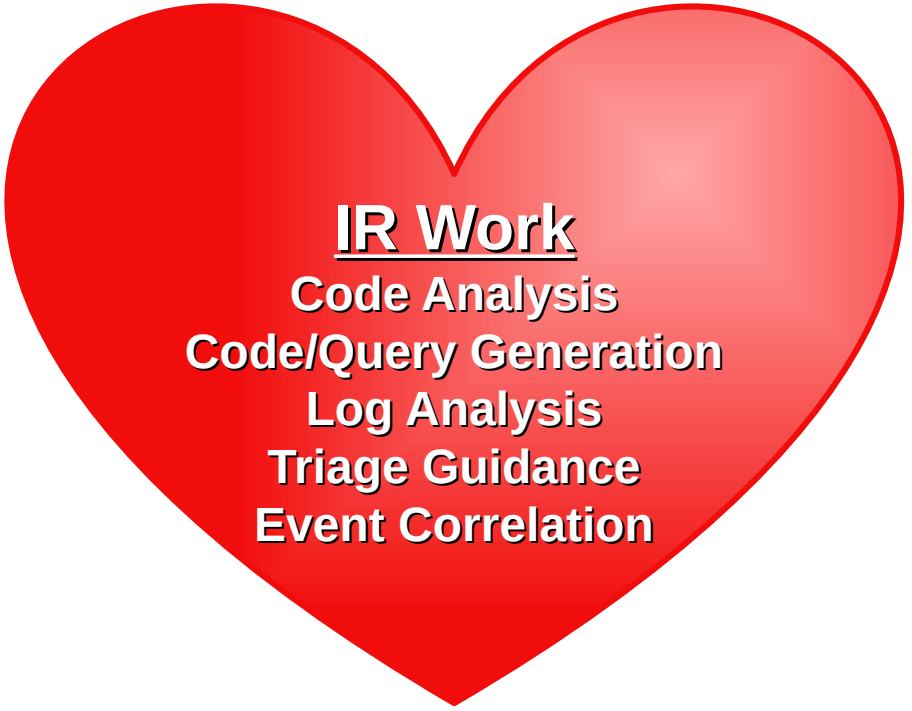
She'd want to paddle Al with a yardstick...



Now,

What I Love about AI!

Ways I've Benefitted

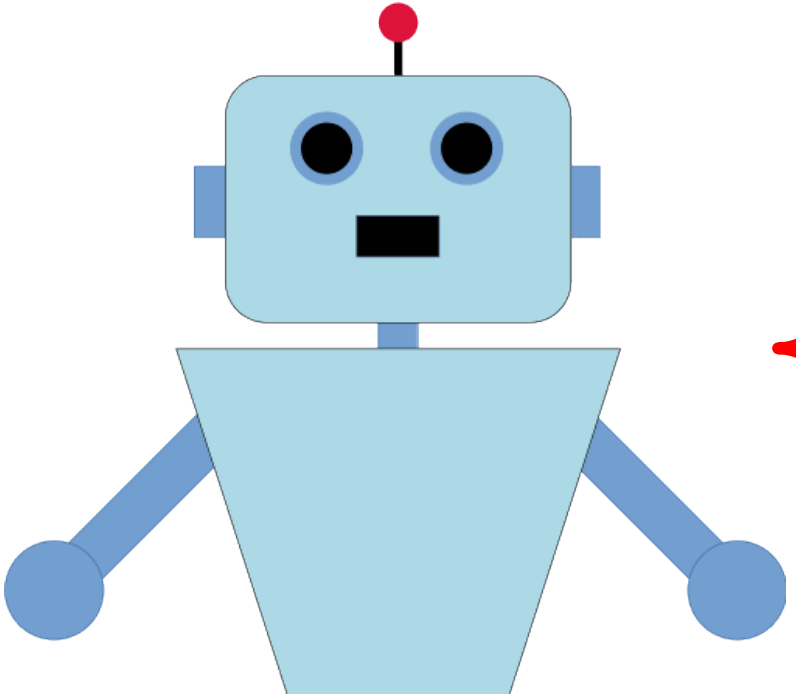


So,

remember this slide from before?

About the Attack Surface

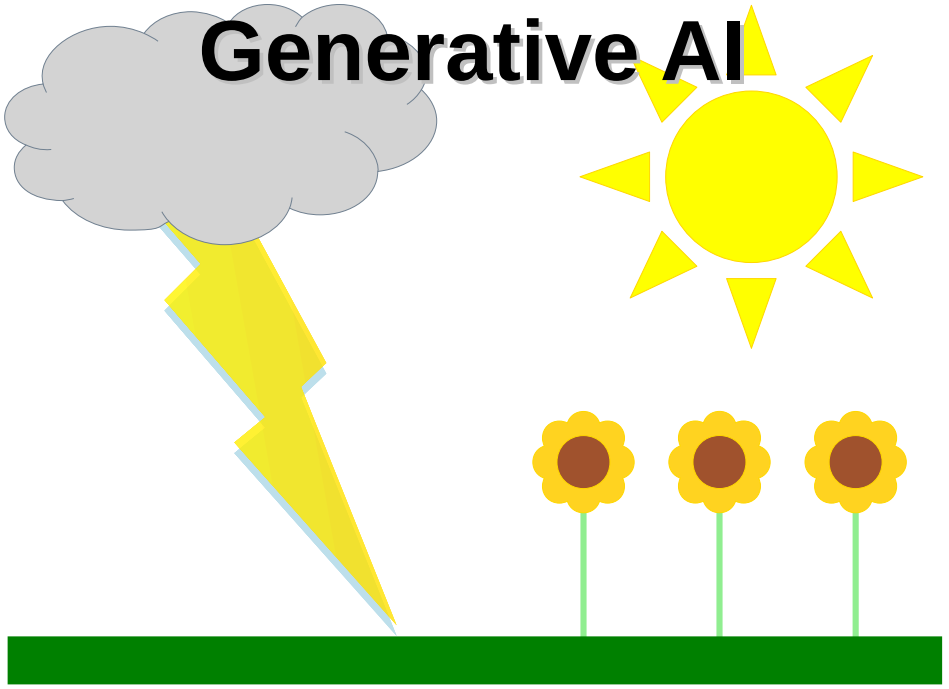
AI-Powered Chat Bot



- Prompt Injection
- Data/Model Poisoning
- Evasion
- Inversion or Extraction
- Etc.

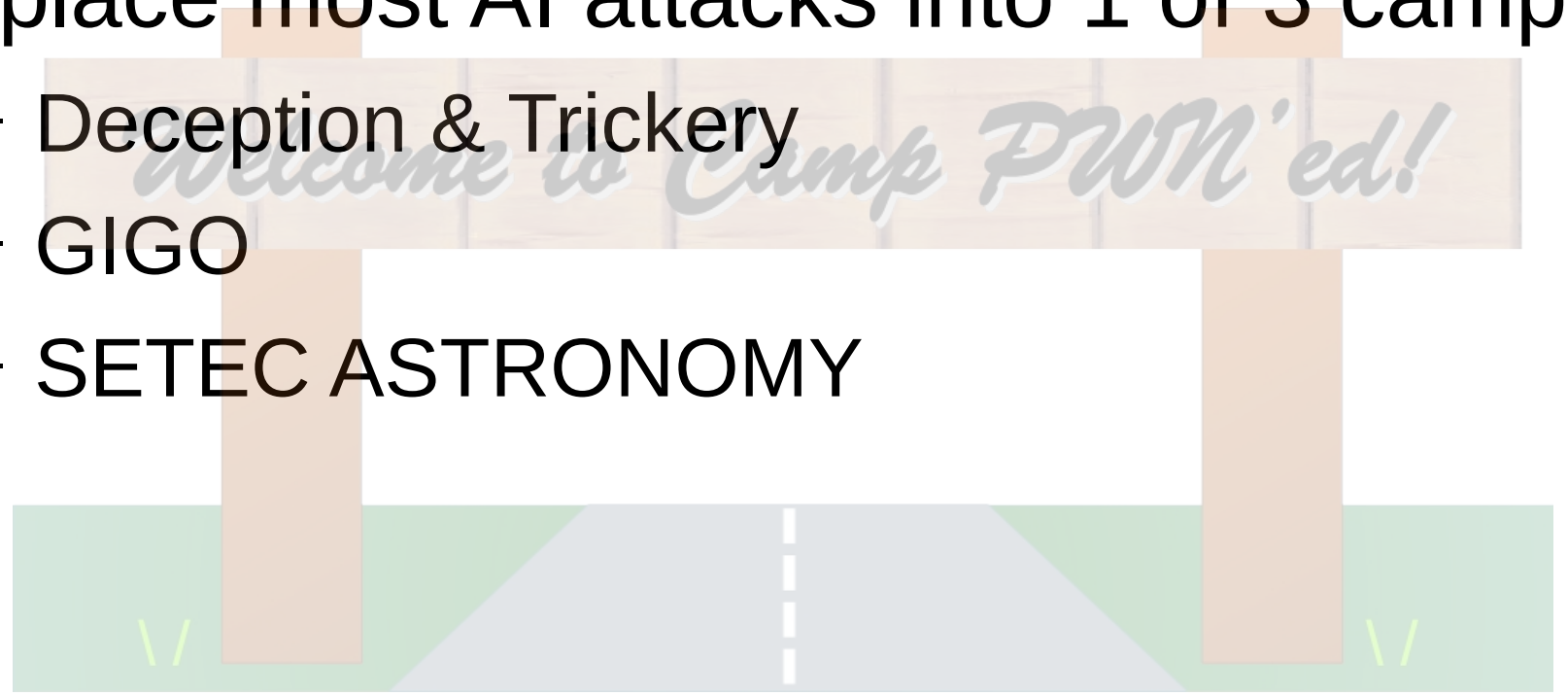
Content Generation

- Social Engineering
  - Phishing
  - Vishing
  - Deep Fakes
  - Etc.



AI Attacks

- I place most AI attacks into 1 of 3 camps
  - Deception & Trickery
  - GIGO
  - SETEC ASTRONOMY

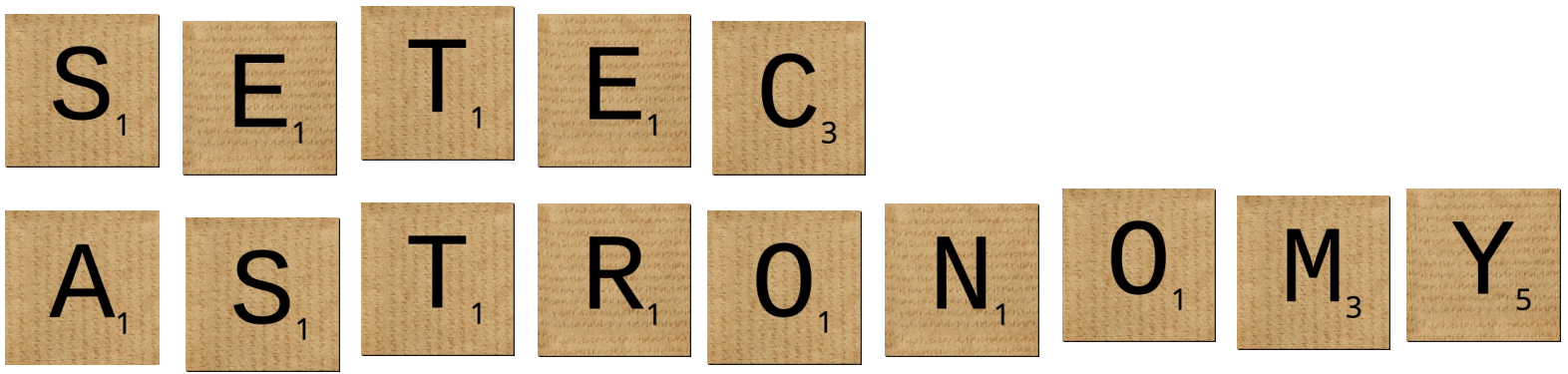


AI Deception & Trickery

AI GIGO

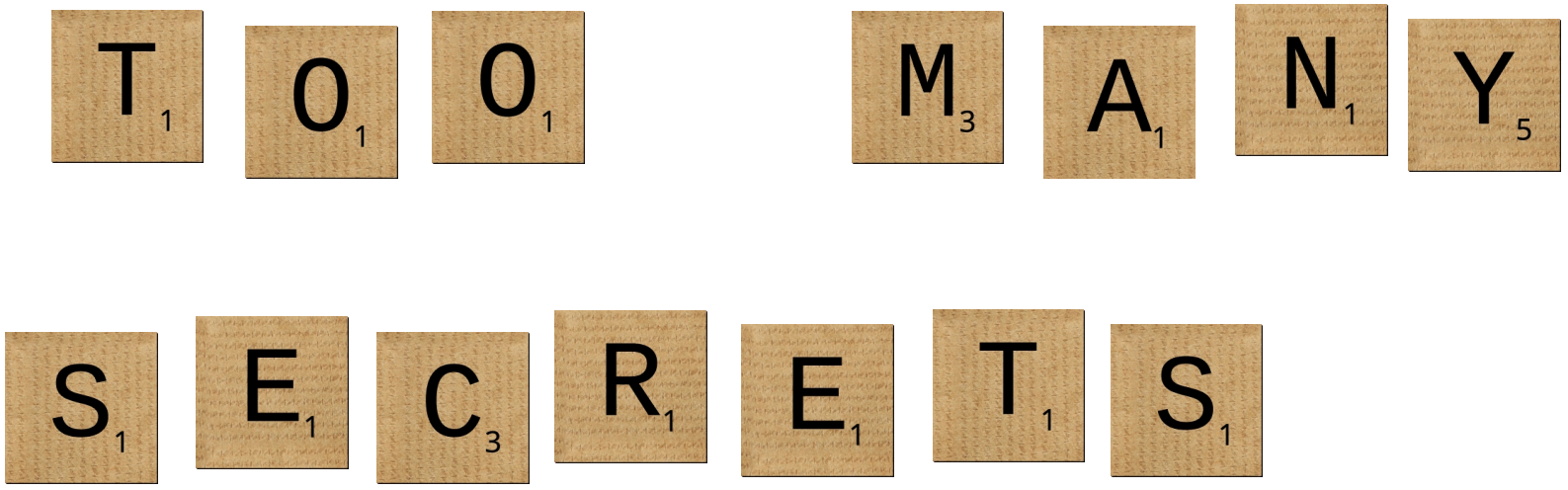
Garbage In = Garbage Out

AI SETEC ASTRONOMY



** Source = "Sneakers" movie*

AI SETEC ASTRONOMY



** Source = "Sneakers" movie*

And,

how about this slide again?

Data Breach (Top Techniques)

1. Ransomware	6. Defense Evasion
2. Stolen Credentials	7. Network Scanning
3. Exploit Vulnerability	8. Exploit Misconfiguration
4. Phishing	9. Data Leakage
5. Backdoor / C2	10. Disable Controls

** Source = 2025 Verizon DBIR*

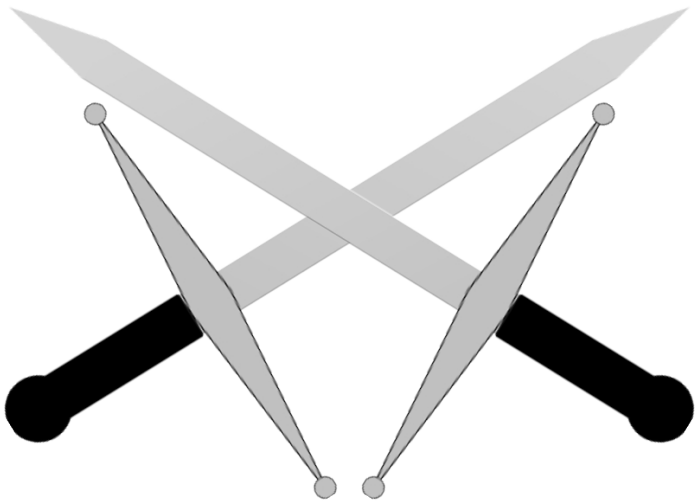
Wrapping Up

I want to close out with this...

Stay on Target

If we're not using AI to solve these same old problems. What are we doing?

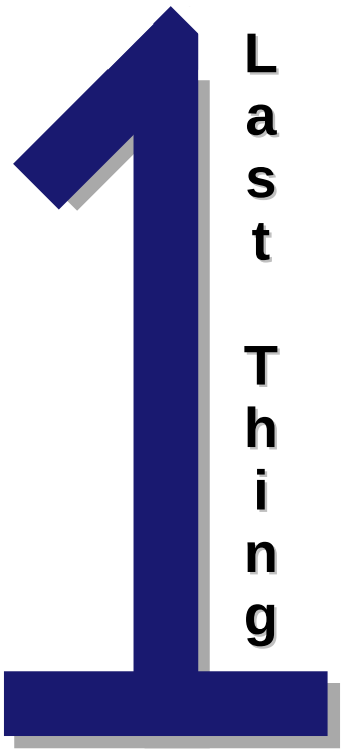
Call to Arms



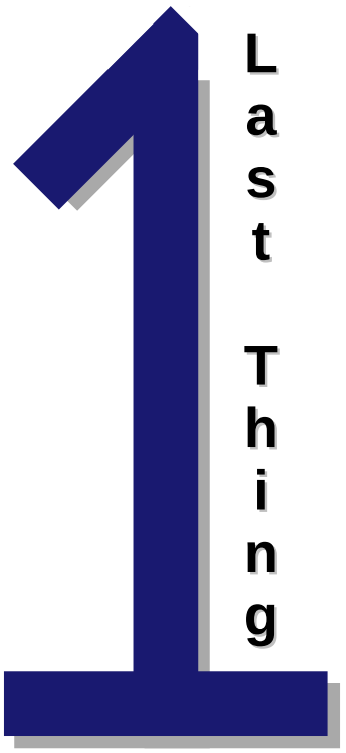
Because

I'm sick and tired of seeing the cyber criminals win!

Oh,

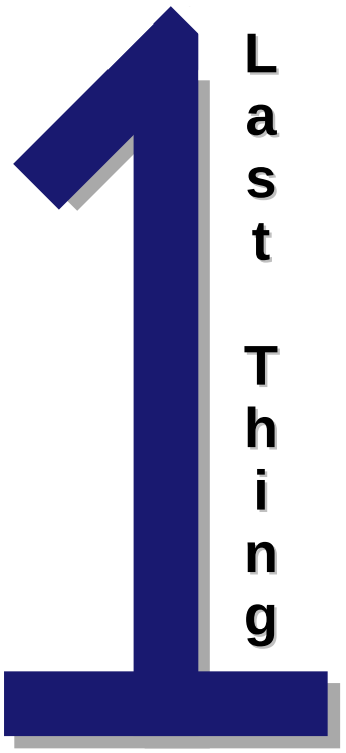


Oh,



Regardless of your Information Security goals and objectives…

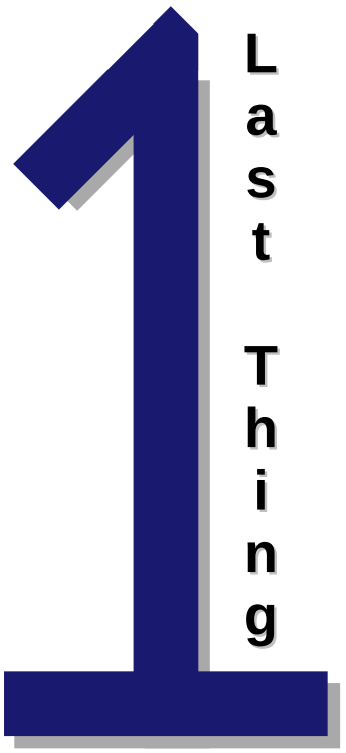
Oh,



Regardless of your Information Security goals and objectives…

If you want to get really good at InfoSec...

Oh,



Regardless of your Information Security goals and objectives…

If you want to get really good at InfoSec...

Learn to "*Think like an attacker!*"

The End

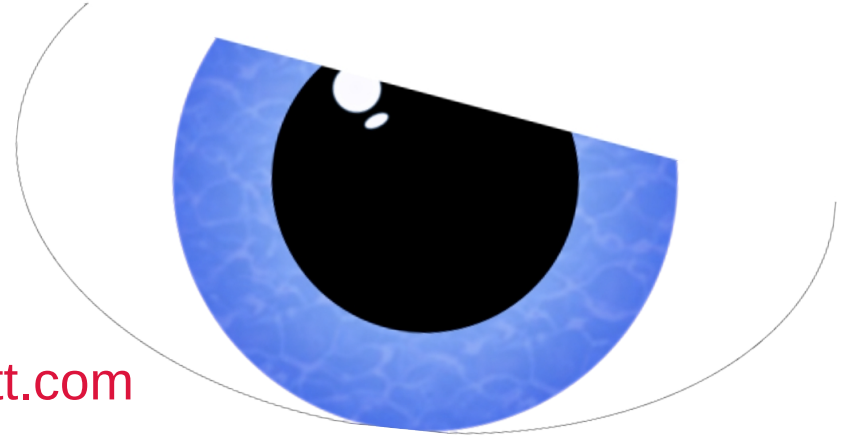
0
0
0
0
0
1
1

0x3

city of CINCINNATI

11/08/2025

PDF http://slides.dfirmatt.com



Eye of the Responder