Stage Crash Course in

KQL

http://slides.dfirmatt.com

About Matt

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

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.

I almost called the talk, this

Inspired by this...

I almost called the talk, this

- but I feared people wouldn’t understand the joke

I almost called the talk, this

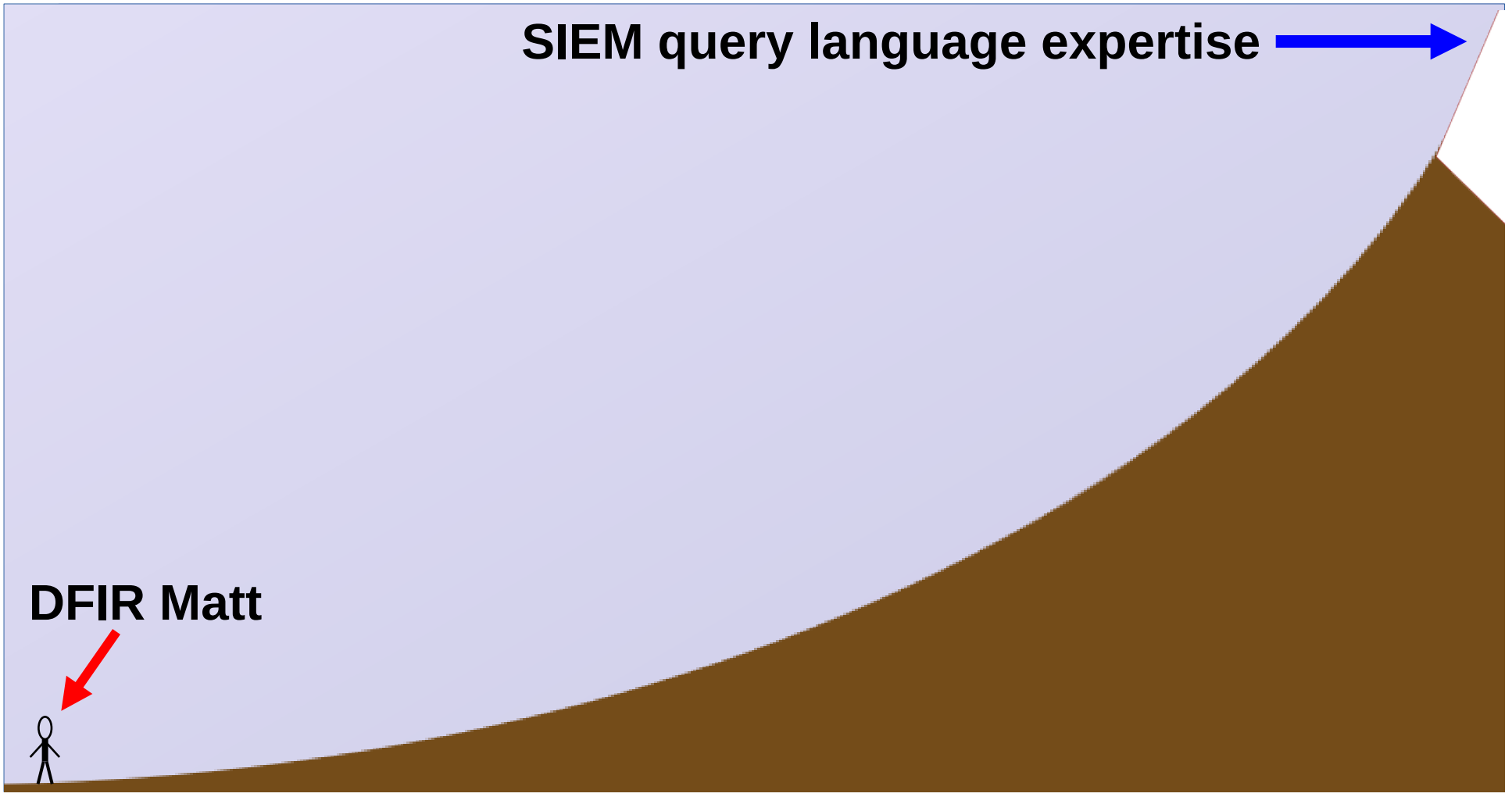
- but I feared people wouldn’t understand the joke
- Not to worry though

I almost called the talk, this

- but I feared people wouldn’t understand the joke
- Not to worry though
  - This is free!

SIEM Query Skill Building

Sometimes the journey begins like this...


SIEM query language expertise
DFIR Matt

Motherly Advice

Motherly Advice

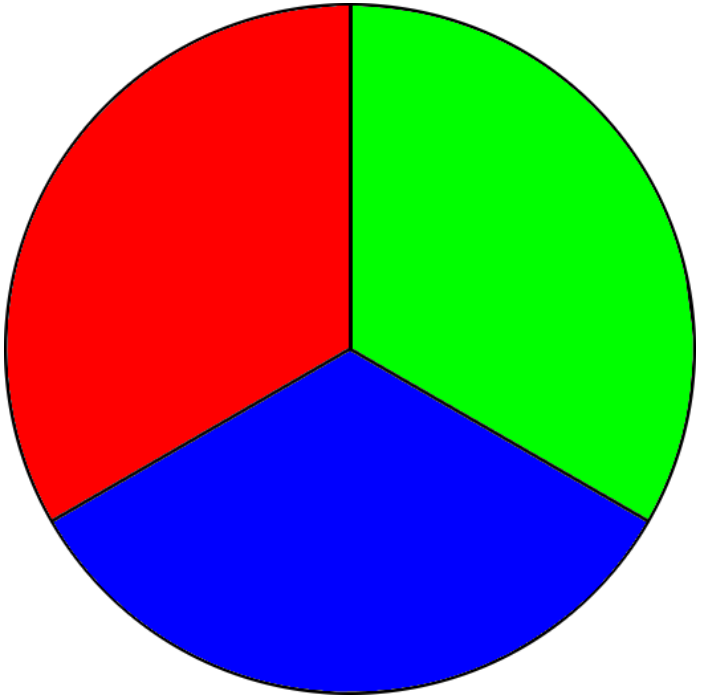
If it was easy, everyone would be doing it...

Final Disclaimer!

Just wanted to remind everyone...

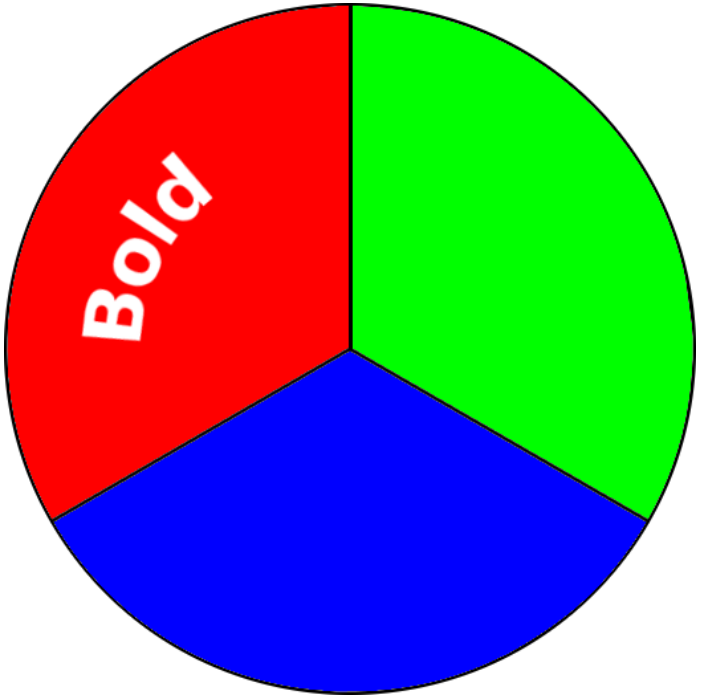
*** Live Demo Alert ***

This presentation features “Live Demos”, because the speaker is...



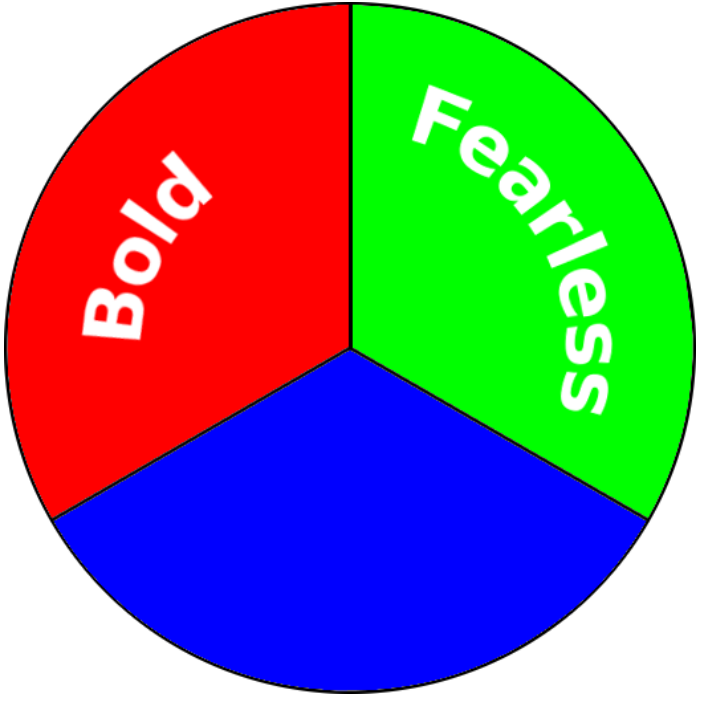
*** Live Demo Alert ***

This presentation features “Live Demos”, because the speaker is...



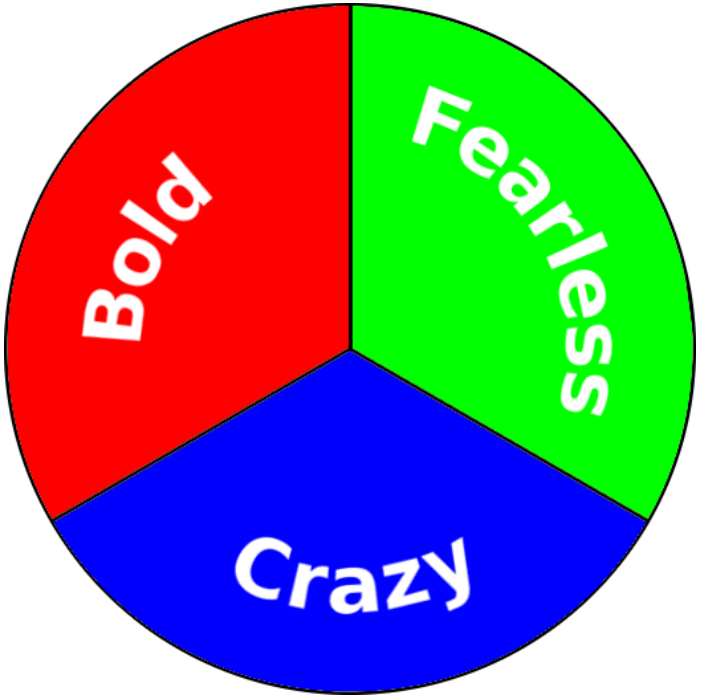
*** Live Demo Alert ***

This presentation features “Live Demos”, because the speaker is...



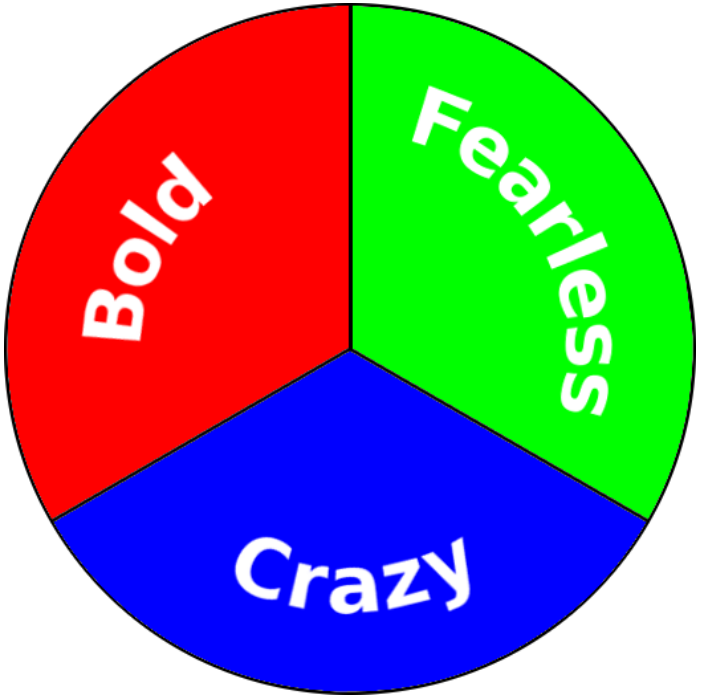
*** Live Demo Alert ***

This presentation features “Live Demos”, because the speaker is...



*** Live Demo Alert ***

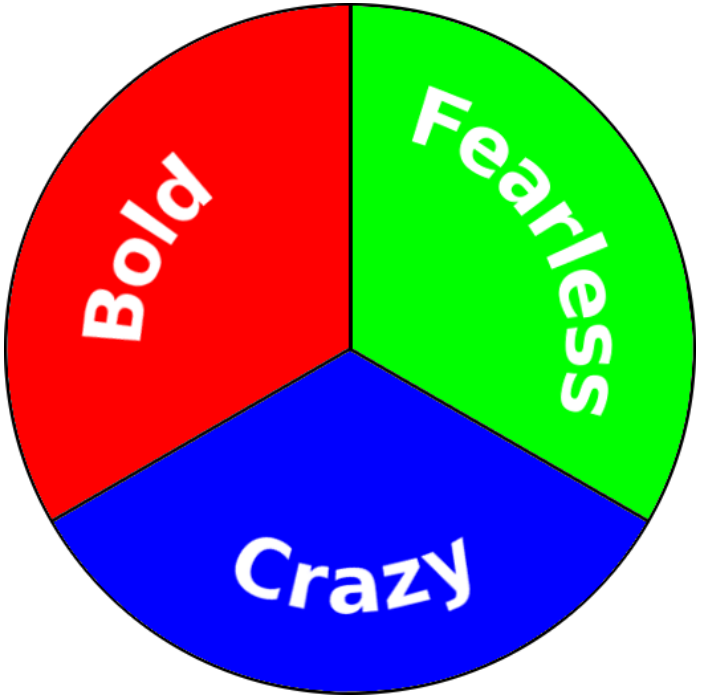
Please pick 2…



*** Live Demo Alert ***

Please pick 2…

So I am not <u>just</u> **Crazy**!



Let’s Begin!

Short Address

http://workshops.dfirmatt.com

Lab Guide (text file inside the ‘kql’ folder)

https://github.com/cerkah/workshops/blob/main/kql/KQL_Lab-Guide_v-0-0-1.txt

Training Platform

https://detective.kusto.io/

The End

Thank you all for attending!
I hope everyone learned something new.

Questions

Who?

What?

When?

Where?

Why?

How?

Stage Crash Course in

KQL

http://slides.dfirmatt.com