Developing Diverse Analysis in Cybersecurity

Introduction

- Cybersecurity enthusiast/professional 10+ years
  - Incident Response team lead
  - Information Systems Security Officer
  - Systems Administrator
- If I had a time machine I would want to be a wizard.
- Curious
- Eagle eyed
- Curious

Incident Response Life Cycle

Figure 3-1 illustrates the incident response life cycle.

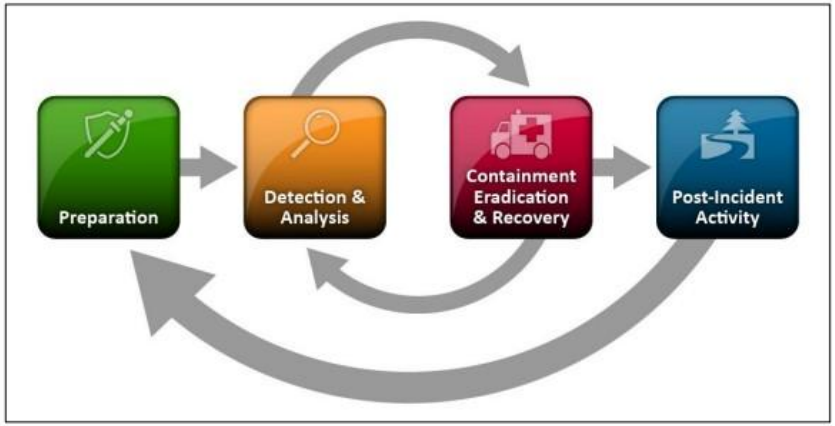
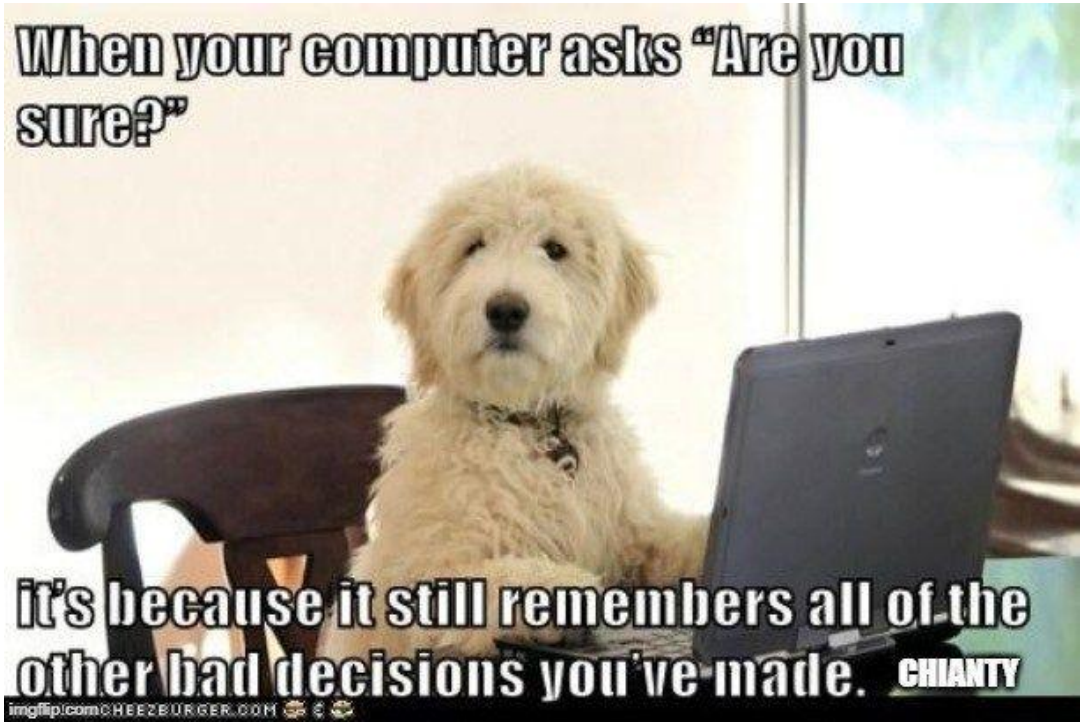


Figure 3-1. Incident Response Life Cycle

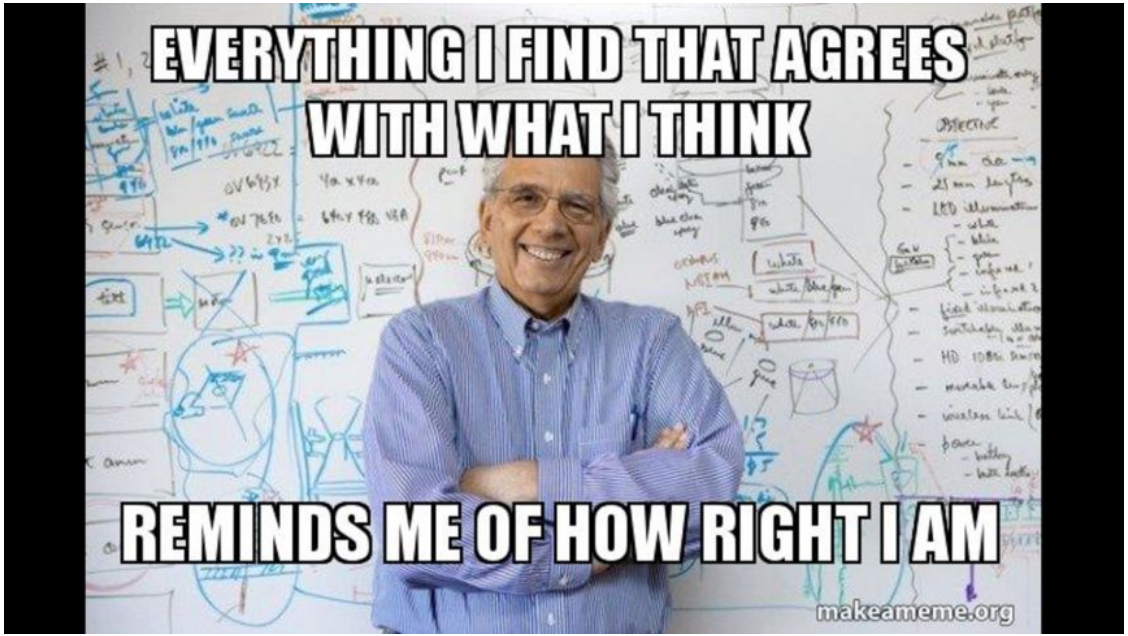
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Cognitive bias impacts critical decision making



Some types of Analysis

Beware of Bias

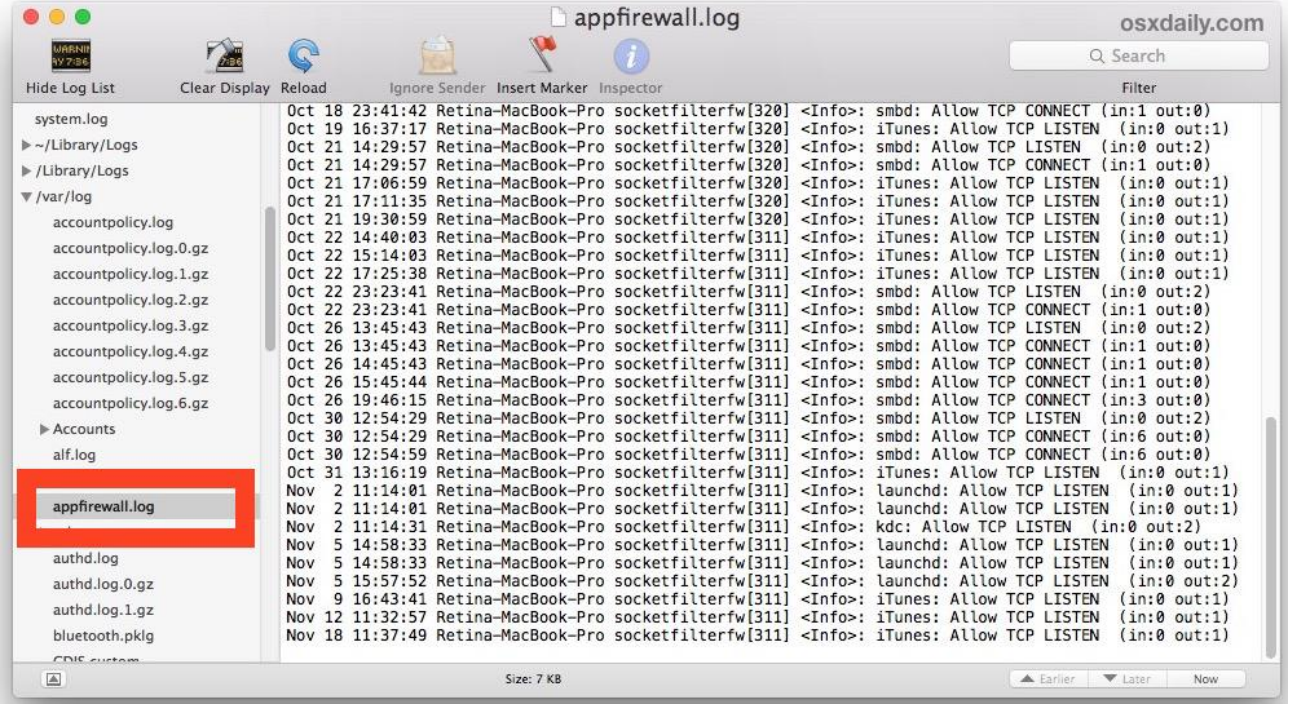


Descriptive

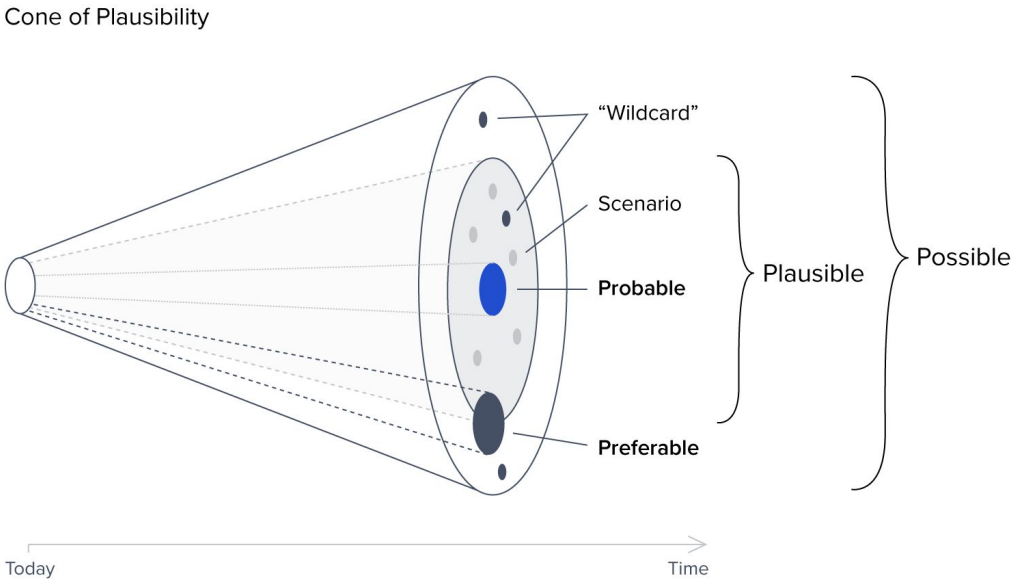
```
top - 18:40:43 up 4 min,  2 users,  load average: 0.52, 0.73, 0.36
Tasks: 165 total,   1 running, 164 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.0 us,  0.0 sy,  0.3 ni, 99.3 id,  0.0 wa,  0.0 hi,  0.3 si,  0.0 st
KiB Mem :  3881880 total,  1898100 free,  1235504 used,   748276 buff/cache
KiB Swap:        0 total,        0 free,        0 used.  2388848 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
 1225 mysql     20   0 1418408 406696  14792 S   1.0 10.5   0:04.28 mysqld
 2166 root      30  10 1177324 270600  10516 S   0.7  7.0   0:05.87 yumBackend.py
  101 root      20   0       0      0      0 S   0.3  0.0   0:00.07 kworker/0:4
  280 root      20   0       0      0      0 S   0.3  0.0   0:00.17 xfsaild/sda1
 1326 root      20   0  479912   5592   4372 S   0.3  0.1   0:00.13 packagekitd
 2175 root      20   0  157716   2232   1544 R   0.3  0.1   0:00.13 top
    1 root      20   0  125344   3868   2496 S   0.0  0.1   0:01.14 systemd
    2 root      20   0       0      0      0 S   0.0  0.0   0:00.00 kthreadd
    3 root      20   0       0      0      0 S   0.0  0.0   0:00.08 ksoftirqd/0
    4 root      20   0       0      0      0 S   0.0  0.0   0:00.00 kworker/0:0
    5 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 kworker/0:0H
    6 root      20   0       0      0      0 S   0.0  0.0   0:00.00 kworker/u2:0
    7 root      rt   0       0      0      0 S   0.0  0.0   0:00.00 migration/0
    8 root      20   0       0      0      0 S   0.0  0.0   0:00.00 rcu_bh
    9 root      20   0       0      0      0 S   0.0  0.0   0:00.19 rcu_sched
   10 root      rt   0       0      0      0 S   0.0  0.0   0:00.00 watchdog/0
   12 root      20   0       0      0      0 S   0.0  0.0   0:00.00 kdevtmpfs
```

Diagnostic

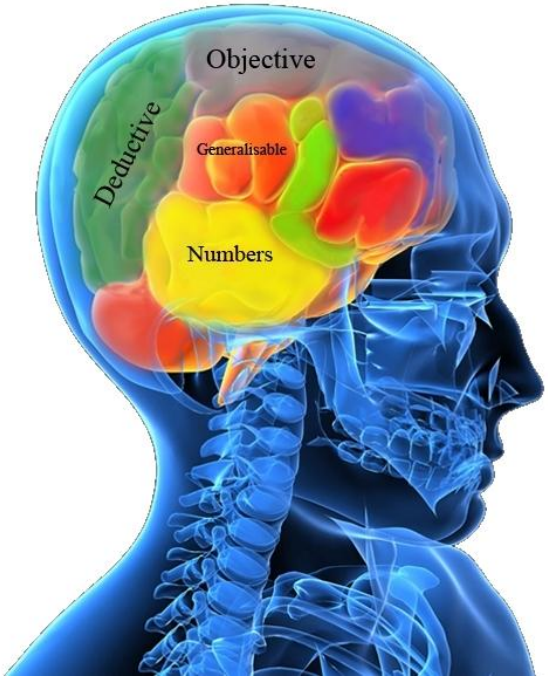

appfirewall.log
osxdaily.com
Hide Log List
Clear Display
Reload
Ignore Sender
Insert Marker
Inspector
Search
Filter
system.log
~/Library/Logs
/Library/Logs
/var/log
accountpolicy.log
accountpolicy.log.0.gz
accountpolicy.log.1.gz
accountpolicy.log.2.gz
accountpolicy.log.3.gz
accountpolicy.log.4.gz
accountpolicy.log.5.gz
accountpolicy.log.6.gz
Accounts
alf.log
appfirewall.log
authd.log
authd.log.0.gz
authd.log.1.gz
bluetooth.pklg
Oct 18 23:41:42 Retina-MacBook-Pro socketfilterfw[320] <Info>: smbd: Allow TCP CONNECT (in:1 out:0)
Oct 19 16:37:17 Retina-MacBook-Pro socketfilterfw[320] <Info>: iTunes: Allow TCP LISTEN (in:0 out:1)
Oct 21 14:29:57 Retina-MacBook-Pro socketfilterfw[320] <Info>: smbd: Allow TCP LISTEN (in:0 out:2)
Oct 21 14:29:57 Retina-MacBook-Pro socketfilterfw[320] <Info>: smbd: Allow TCP CONNECT (in:1 out:0)
Oct 21 17:06:59 Retina-MacBook-Pro socketfilterfw[320] <Info>: iTunes: Allow TCP LISTEN (in:0 out:1)
Oct 21 17:11:35 Retina-MacBook-Pro socketfilterfw[320] <Info>: iTunes: Allow TCP LISTEN (in:0 out:1)
Oct 21 19:30:59 Retina-MacBook-Pro socketfilterfw[320] <Info>: iTunes: Allow TCP LISTEN (in:0 out:1)
Oct 22 14:40:03 Retina-MacBook-Pro socketfilterfw[311] <Info>: iTunes: Allow TCP LISTEN (in:0 out:1)
Oct 22 15:14:03 Retina-MacBook-Pro socketfilterfw[311] <Info>: iTunes: Allow TCP LISTEN (in:0 out:1)
Oct 22 17:25:38 Retina-MacBook-Pro socketfilterfw[311] <Info>: iTunes: Allow TCP LISTEN (in:0 out:1)
Oct 22 23:23:41 Retina-MacBook-Pro socketfilterfw[311] <Info>: smbd: Allow TCP LISTEN (in:0 out:2)
Oct 22 23:23:41 Retina-MacBook-Pro socketfilterfw[311] <Info>: smbd: Allow TCP CONNECT (in:1 out:0)
Oct 26 13:45:43 Retina-MacBook-Pro socketfilterfw[311] <Info>: smbd: Allow TCP LISTEN (in:0 out:2)
Oct 26 13:45:43 Retina-MacBook-Pro socketfilterfw[311] <Info>: smbd: Allow TCP CONNECT (in:1 out:0)
Oct 26 14:45:43 Retina-MacBook-Pro socketfilterfw[311] <Info>: smbd: Allow TCP CONNECT (in:1 out:0)
Oct 26 15:45:44 Retina-MacBook-Pro socketfilterfw[311] <Info>: smbd: Allow TCP CONNECT (in:1 out:0)
Oct 26 19:46:15 Retina-MacBook-Pro socketfilterfw[311] <Info>: smbd: Allow TCP CONNECT (in:3 out:0)
Oct 30 12:54:29 Retina-MacBook-Pro socketfilterfw[311] <Info>: smbd: Allow TCP LISTEN (in:0 out:2)
Oct 30 12:54:29 Retina-MacBook-Pro socketfilterfw[311] <Info>: smbd: Allow TCP CONNECT (in:6 out:0)
Oct 30 12:54:59 Retina-MacBook-Pro socketfilterfw[311] <Info>: smbd: Allow TCP CONNECT (in:6 out:0)
Oct 31 13:16:19 Retina-MacBook-Pro socketfilterfw[311] <Info>: iTunes: Allow TCP LISTEN (in:0 out:1)
Nov 2 11:14:01 Retina-MacBook-Pro socketfilterfw[311] <Info>: launchd: Allow TCP LISTEN (in:0 out:1)
Nov 2 11:14:01 Retina-MacBook-Pro socketfilterfw[311] <Info>: launchd: Allow TCP LISTEN (in:0 out:1)
Nov 2 11:14:31 Retina-MacBook-Pro socketfilterfw[311] <Info>: kdc: Allow TCP LISTEN (in:0 out:2)
Nov 5 14:58:33 Retina-MacBook-Pro socketfilterfw[311] <Info>: launchd: Allow TCP LISTEN (in:0 out:1)
Nov 5 14:58:33 Retina-MacBook-Pro socketfilterfw[311] <Info>: launchd: Allow TCP LISTEN (in:0 out:1)
Nov 5 15:57:52 Retina-MacBook-Pro socketfilterfw[311] <Info>: launchd: Allow TCP LISTEN (in:0 out:2)
Nov 9 16:43:41 Retina-MacBook-Pro socketfilterfw[311] <Info>: iTunes: Allow TCP LISTEN (in:0 out:1)
Nov 12 11:32:57 Retina-MacBook-Pro socketfilterfw[311] <Info>: iTunes: Allow TCP LISTEN (in:0 out:1)
Nov 18 11:37:49 Retina-MacBook-Pro socketfilterfw[311] <Info>: iTunes: Allow TCP LISTEN (in:0 out:1)
Size: 7 KB
Earlier
Later
Now

Predictive

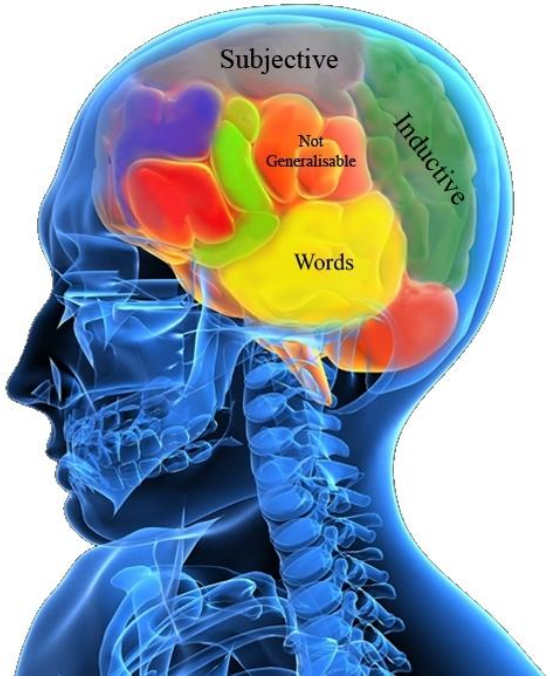


https://www.toptal.com/insights/innovation/strategic-foresight-zalman

Quantitative



Qualitative



Analysis of Competing Hypotheses (ACH)

- Hypothesis
- Evidence
- Matrix
- Refinement
- Evaluation

Hypothesis

- Identify multiple hypotheses by a single analyst or a group of analysts.
- Gather a reasonable number and begin screening them to find the best hypothesesis.

Evidence

- Broadly examine selected hypothesis and create a list of evidence for each.
- Compare and evaluate evidence critically

Matrix

- Create a matrix to diagnose hypotheses utilizing collected evidence.

Refinement

- Evaluate if evidence is incomplete or if new hypothesis need to be proposed.
- Maintain documentation of all evidence including that which will be excluded at this stage.
- Strive to prove each hypothesis wrong rather than proving them right.

Evaluation

- Double-check evidence so that conclusions have more validity.
- Determine credibility of the hypothesis document conclusions and outline potential indicators of compromise to aid future analysis
- Deliver to management.

A tale of two dogs

Lovely Labrador

Calculating Corgi

ACH Matrix

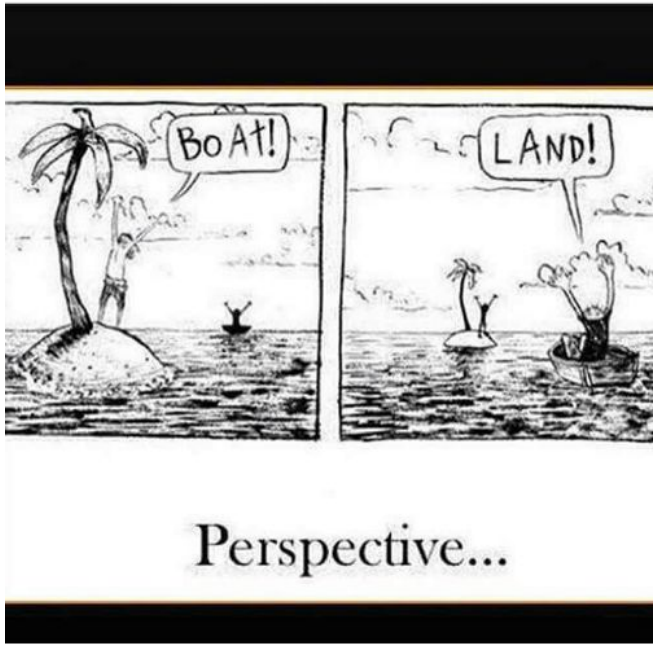
Analysis of Competing Hypothesis Example			
Number	Hypothesis	Evidence	**Credibility**
1	Lovely Labrador got into the garbage can.	This is a known behavior of Lovely Labrador. Won't make eye contact.	H
2	Calculating Corgi stole containers from Recycling.	Recycling is lower to the ground. Significant teeth marks.	M
3	Lovely Labrador and Calculating Corgi worked together.	It's been very quiet in the kitchen.	M
4	Child #1 left food on table and it was removed by Lovely Labrador.	We just had lunch?	L

The most probable answer is generally the one with the least evidence against it

Timeline analysis

How I started

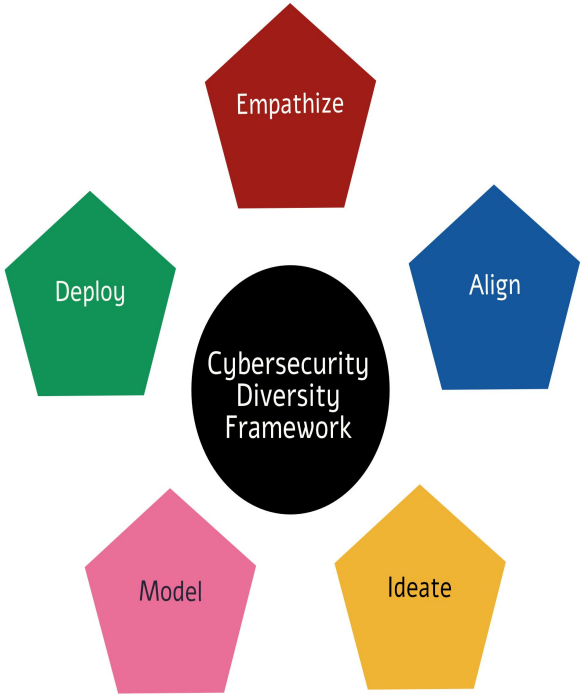
This gets better if...we talk about elephants



“We need diversity if we are to change, grow, and innovate”

—Dr. Katherine W. Phillips

What I do now

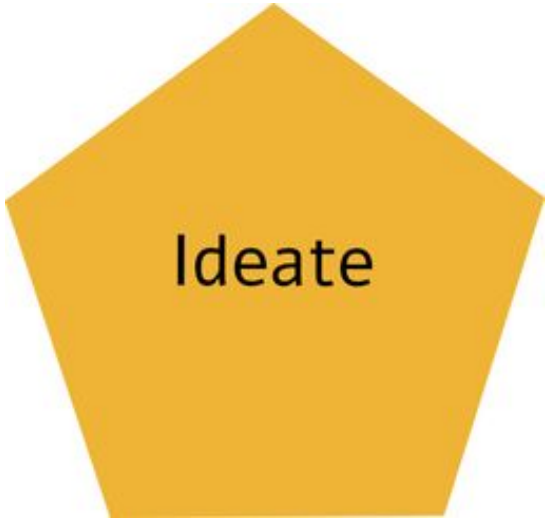

Empathize
Deploy
Align
Cybersecurity Diversity Framework
Model
Ideate

Cyber Diversity Analysis Framework

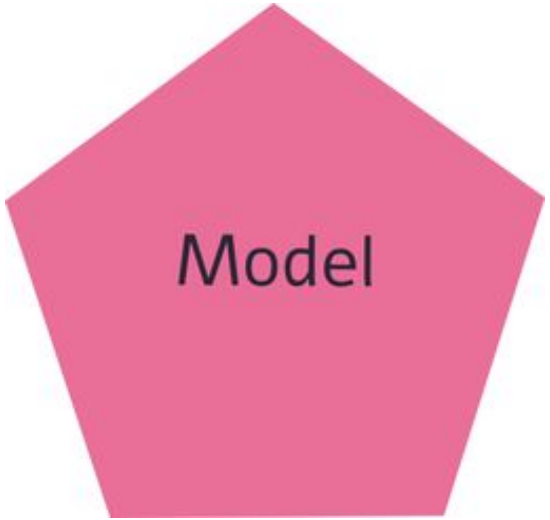
- **Empathize and imagine.**
  What other perspectives are there besides my own?
- **Align your focus.**
  What is known? What is unknown? What tools are needed? What policies and procedures do we follow?
- **Ideate and design solutions.**
  What skills do we have?
- **Model and assess together.**
  How does my thinking need to transform?
- **Deploy the best model.**
  What works? What doesn't work?

- **Empathize and imagine.**
  What other perspectives are there besides my own?

- **Align your focus.**
  What is known? What is unknown? What tools are needed? What policies and procedures do we follow?



- **Ideate and design solutions.**
  What skills do we have?



- **Model and assess together.**
  How does my thinking need to transform?

- **Deploy the best model.**
  What works? What doesn't work?

The Future Partnership of Person and Machine