

How to Build a SOC in Reality



Who Am I

Lauren, GCIH, GMON, CISSP, SOCaaS @lil_lost

- Lots of acronyms
- 15+ yrs IT and Security experience
- Builder of Programs
- Corgi herder
- Unicorn
- Super Power: Ability to manage 3 levels up at all times



WHY?!



It's All Too Much WHAT DO YOU DO



So you wanna build a SOC

Everyone will tell you how

- <https://www.mitre.org/publications/all/ten-strategies-of-a-world-class-cybersecurity-operations-center>
- <https://cybersecurity.att.com/resource-center/ebook/how-to-build-a-security-operations-center>
- <https://logrhythm.com/blog/7-steps-to-build-your-security-operations-center/>
- <https://blog.rapid7.com/2016/06/07/how-to-structure-a-security-operations-center/>
- <https://www.exabeam.com/security-operations-center/how-to-build-a-modern-soc/>

So you wanna build a SOC

Everyone will tell you how

- Designing and Building a Security Operation Center by David Nathans
- Crafting the Infosec Playbook by Jeff Bollinger, Brandon Enright and Matthew Valites
- Security Operations Center: Building Operating and Maintaining your SOC by Joseph Muniz, Gary McIntyre and Nadhem Al Fardan
- Defensive Security Handbook by Lee Brotherson and Amanda Berlin

1. Mission
2. People
3. Inventory
4. Processes
5. Tools

Have a Mission



Have a Mission

What do we do?

Whom do we serve?

How do we serve
them?

What a Mission Looks Like

What level of response will you provide?

Is this a function of the SOC?

Or are there other security teams?

What will you outsource?

Hire People



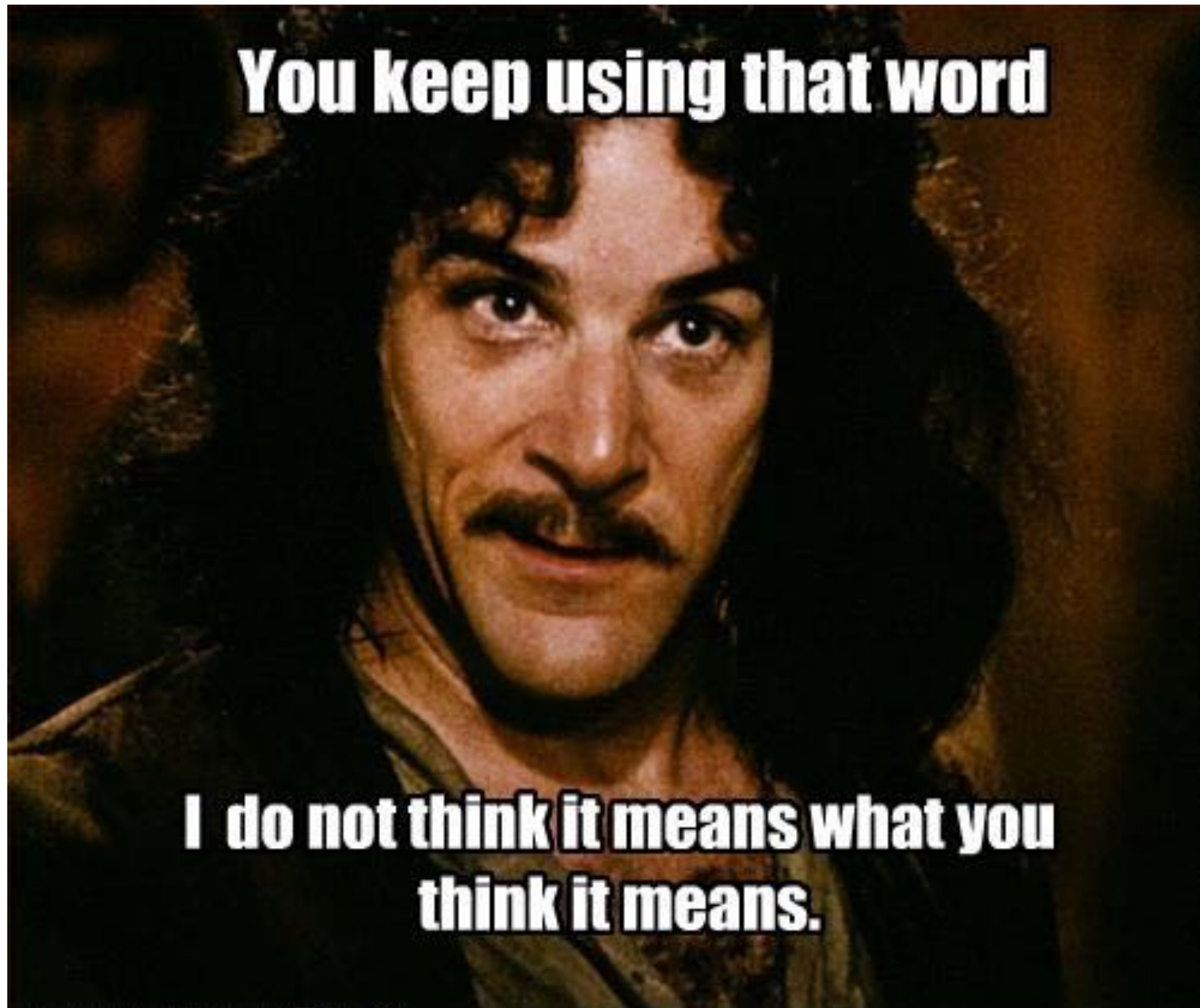
Hire People



Hire People



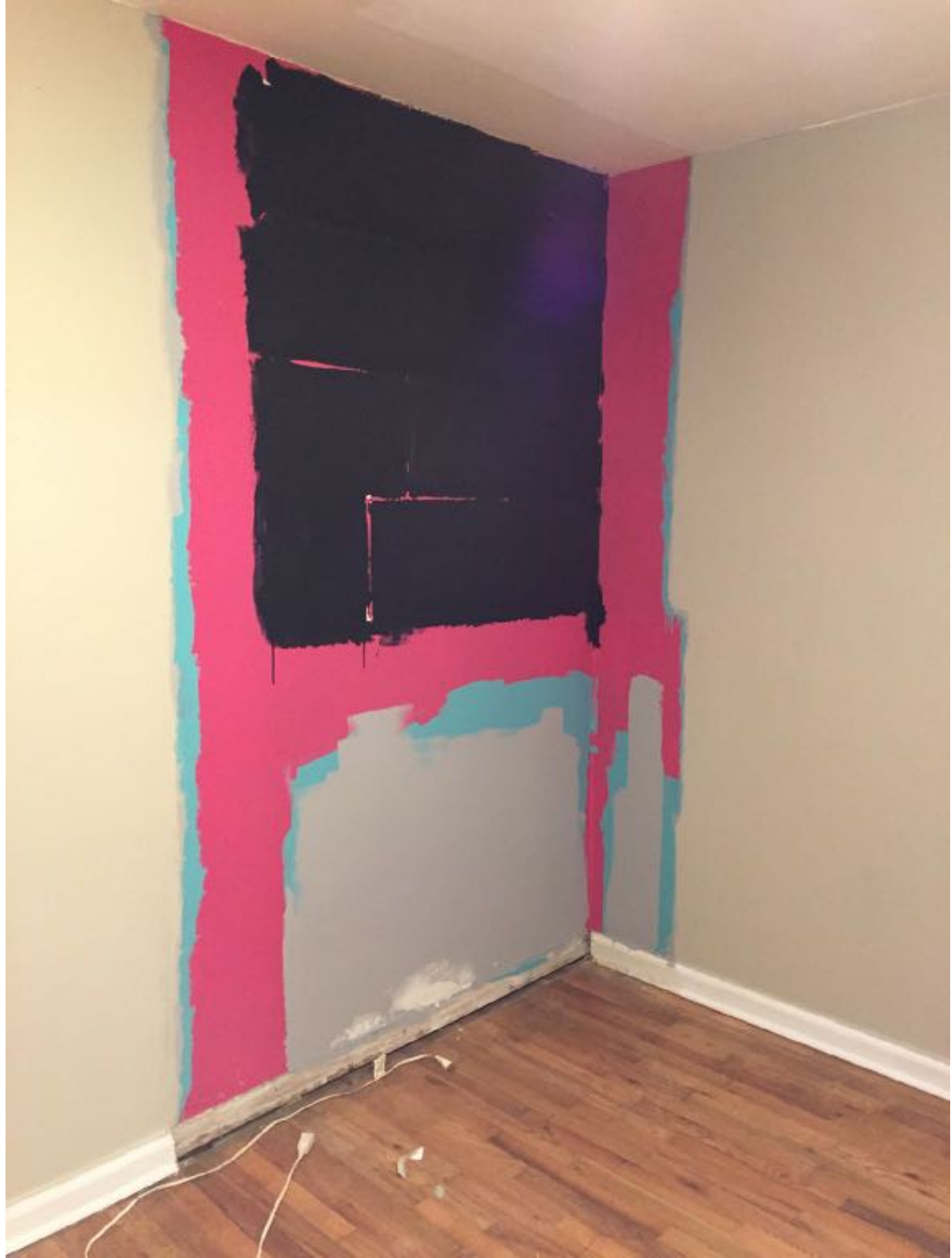
Inventory



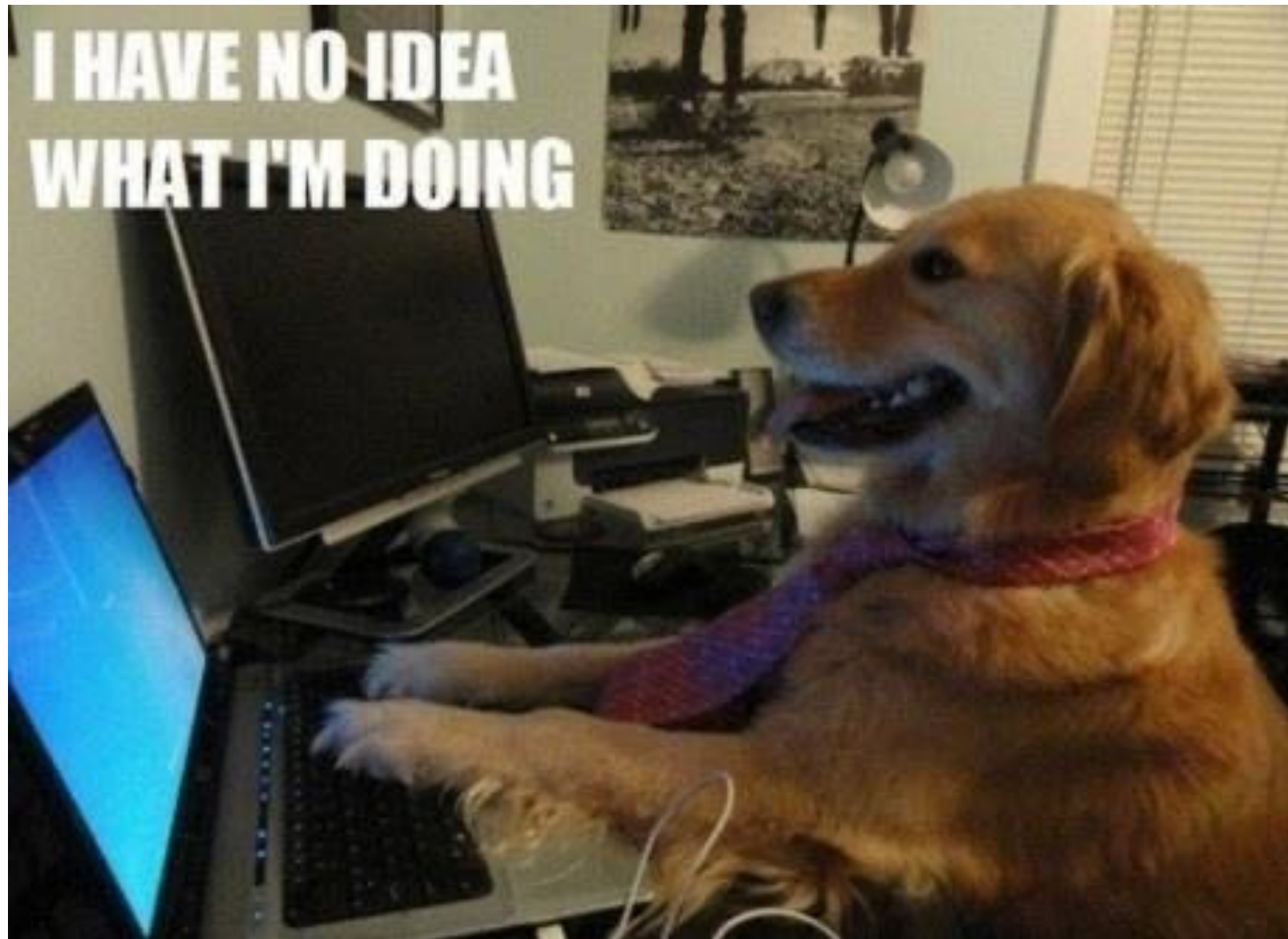


Ways to find the ugly

- NMAP
- Rumble.Run
- SCCM (or other remote mgmt tool)
- Hypervisor reports
- Network Maps



Now Organize it



Now Organize it



Can you find the Crown Jewels?



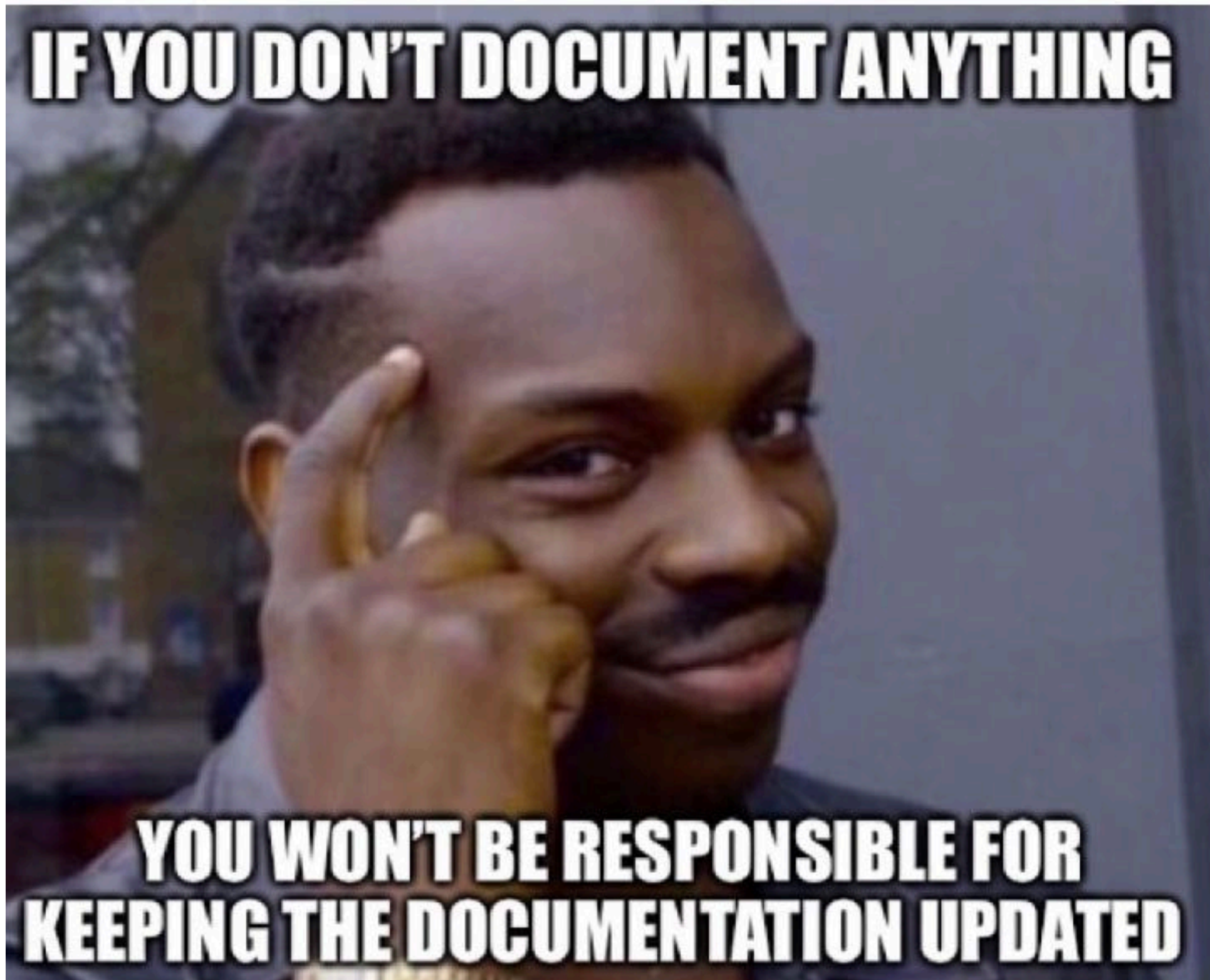
All the Processes





SOC Analysts without processes

WRITE IT DOWN!!!!



Tools



Tools

- Knowledge Management (AKA Wiki)
- Ticketing System (hopefully not email)
- Log Management (or you will hate life)
- Inventory (hopefully someone else problem)
- Automation (makes lives easier)
- All the IR & other tools (based on your mission)

Knowledge Management



Ticketing System



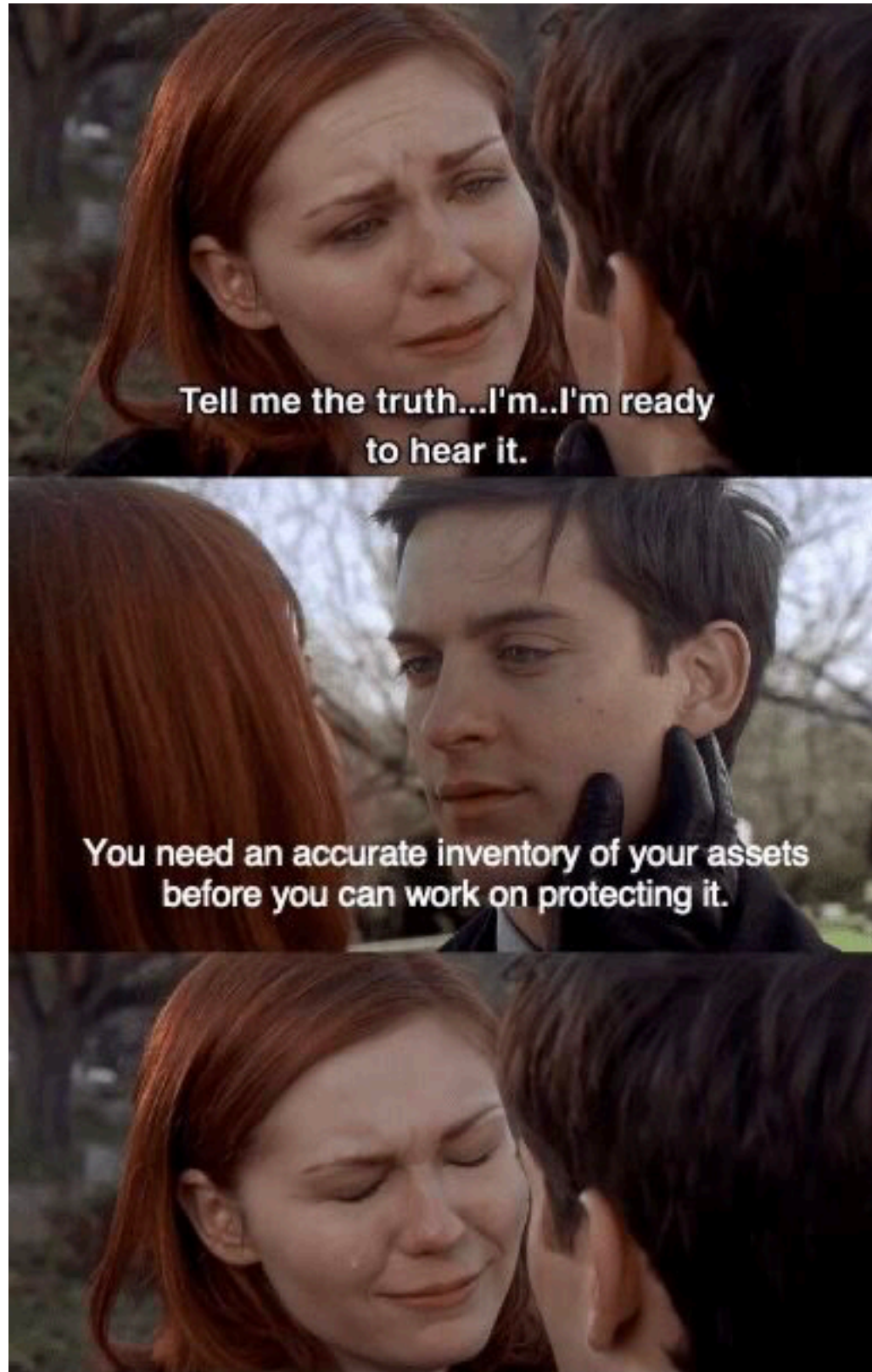
Log Management



Inventory



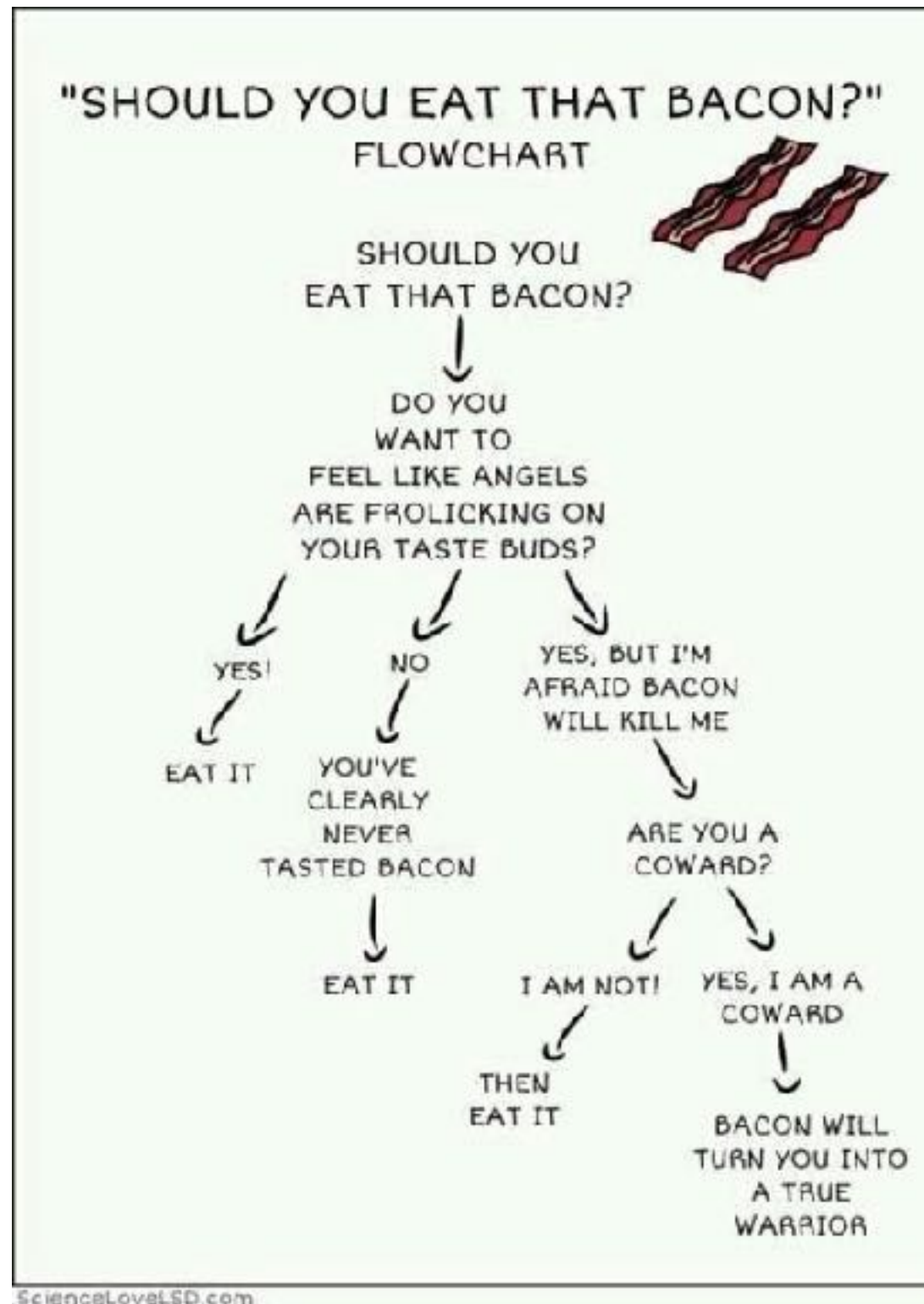
Inventory



Automation



Automation



Automation



ANOMALY DETECTED



IS THIS PIZZA? Y/N

MOAR TOOLZ!

GRR (Google Rapid Response)

Redline

Volatility

The HIVE

Powershell

OS Query

Any.Run

Virus Total

Zeke

OSSEC

sysmon

Memorize

Rekall

Wireshark

Cuckoo

Joe Sandbox

Demisto

strings

Moloch

Cyphon

Threat Crowd

Resource Hacker



AMARI

SOUP

OF THE

DAY



WHISKEY