

# I SLICED MY SIEM

Finally Getting Value out of your SIEM!

@Mag1cM0n



**THANK YOU!**

memegenerator.net



**THANK YOU!**

memegenerator.net

<https://www.cyberwayfinder.com/>



**IM SORRY**

**I DIDNT MEAN TO**


memecrunch.com



**THANK YOU!**

memegenerator.net

# THE PRESENTER

- \$whoami
- @Mag1cM0n 
- 10+ years in Cyber Security;
- I'm kind of purple teamer;



DECATHLON



SOCIETE  
GENERALE



AIRBUS



BNP PARIBAS  
FORTIS

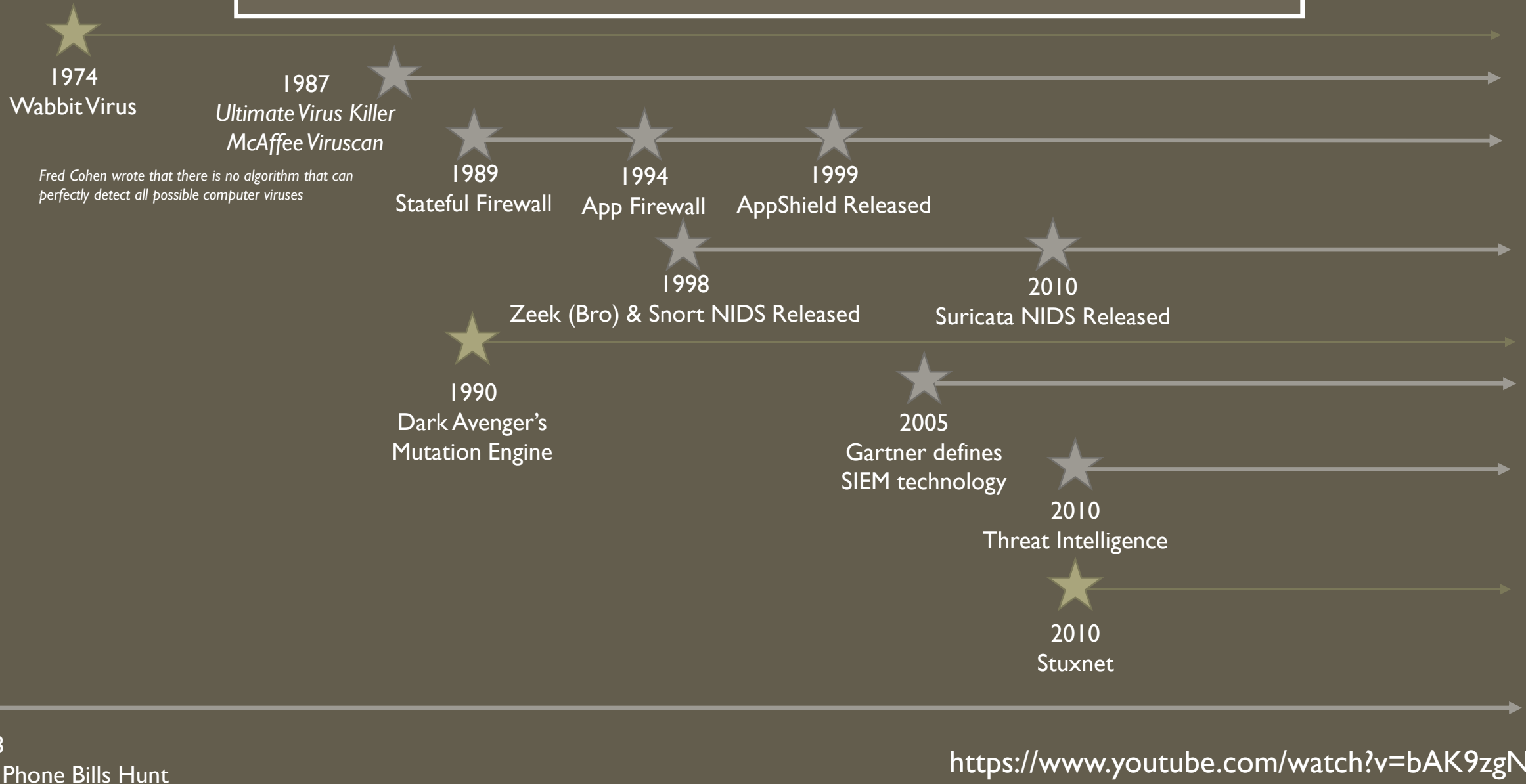


MSSP

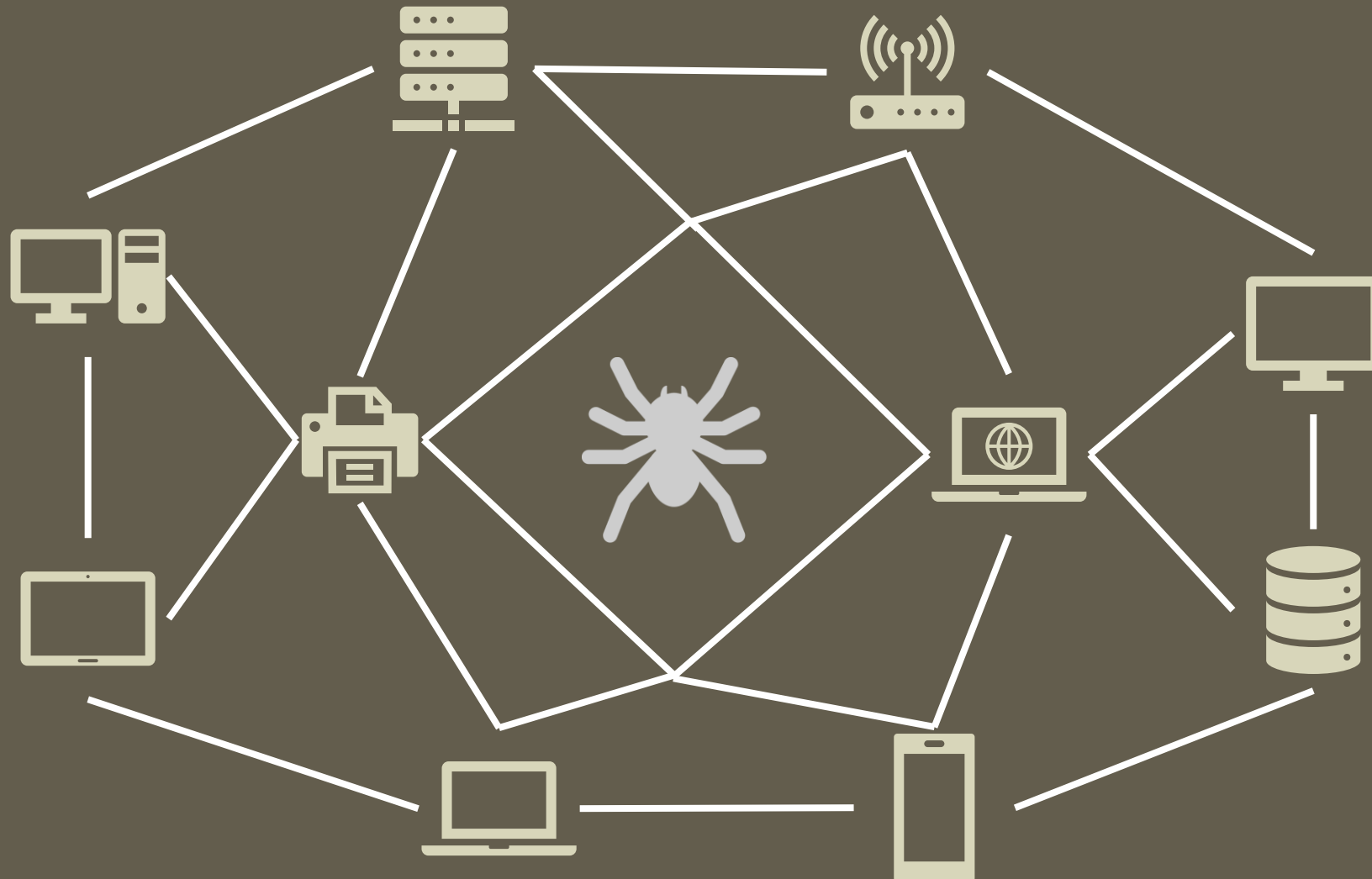
## DISCLAIMER

All opinions expressed during this presentation are mine and do not represent by any means the opinions of my current employer.

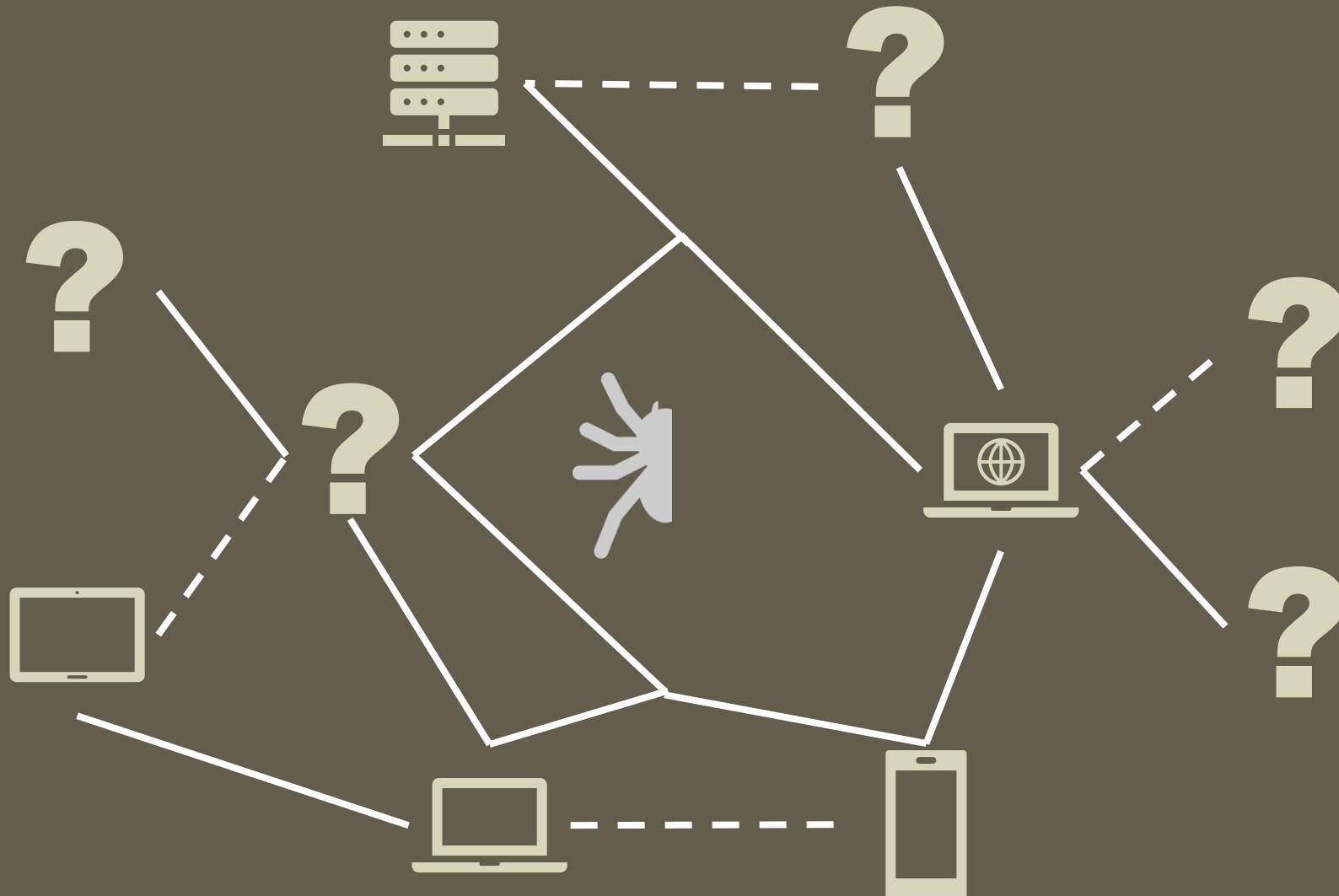
# A (VERY) SHORT HISTORY OF OUR INDUSTRY



# THE SPIDER ANALOGY



# THE SPIDER ANALOGY



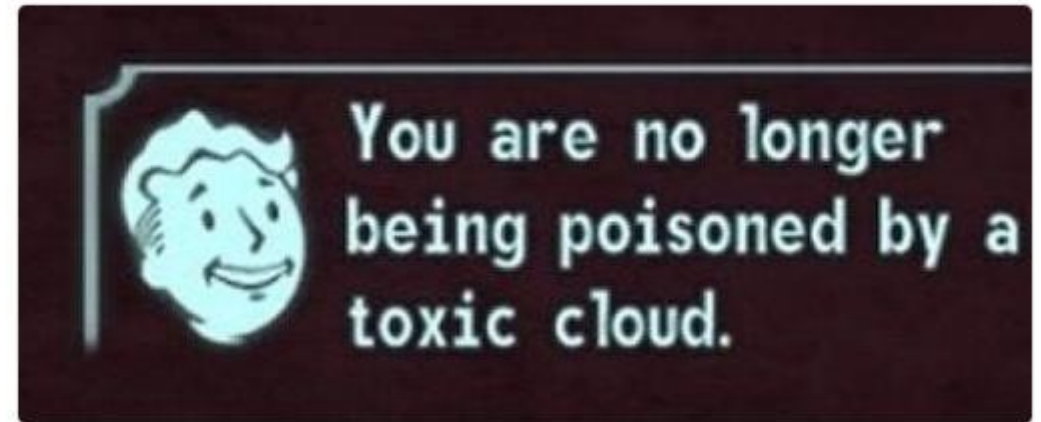
# WHERE THIS TALK COME FROM?

expel<sup>®</sup>

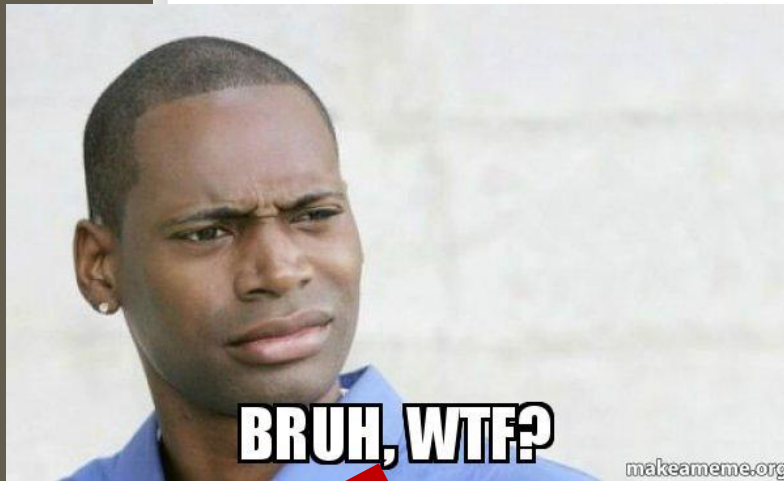


Jack Rhysider @JackRhysider · Sep 10

After you get rid of that SIEM you struggled for 3 years to get running but never offered you any value. #siem #infosec



2 11 32



makeameme.org

Security operations | 6 min read | May 23, 2018 | by Dan Whalen and Lori Easterly | Tags: Management, SIEM, SOC, Tools

How to identify when you've lost control of your SIEM (and how to rein it back in)



# PROCESS IS A SOLUTION



**Dr. Anton Chuvakin**  @anton\_chuvakin · Aug 2

Org: "HELP! My SIEM deployment failed! We hear #SIEM is old/dead tech ..."  
Analyst: "Well, have you tried using it!"  
Org: "Say what? I installed it, isn't it enough?" #random #totallyfake #madeup  
#artificial #nottrue #nope



9



31



97



**Derek Armstrong** @dsplice · Aug 2

Replying to @anton\_chuvakin

Like far too many infosec projects. Most security issues are first a people and process problem. Technology is a DISTANT third!



2



6



**BCC** @BlueCollarCyber · Aug 2

Replying to @anton\_chuvakin

"We have EVERY device logging to SIEM at Debug kevel for PCI, why aren't we stopping phishing and finding APT?" #peopleproblem



2



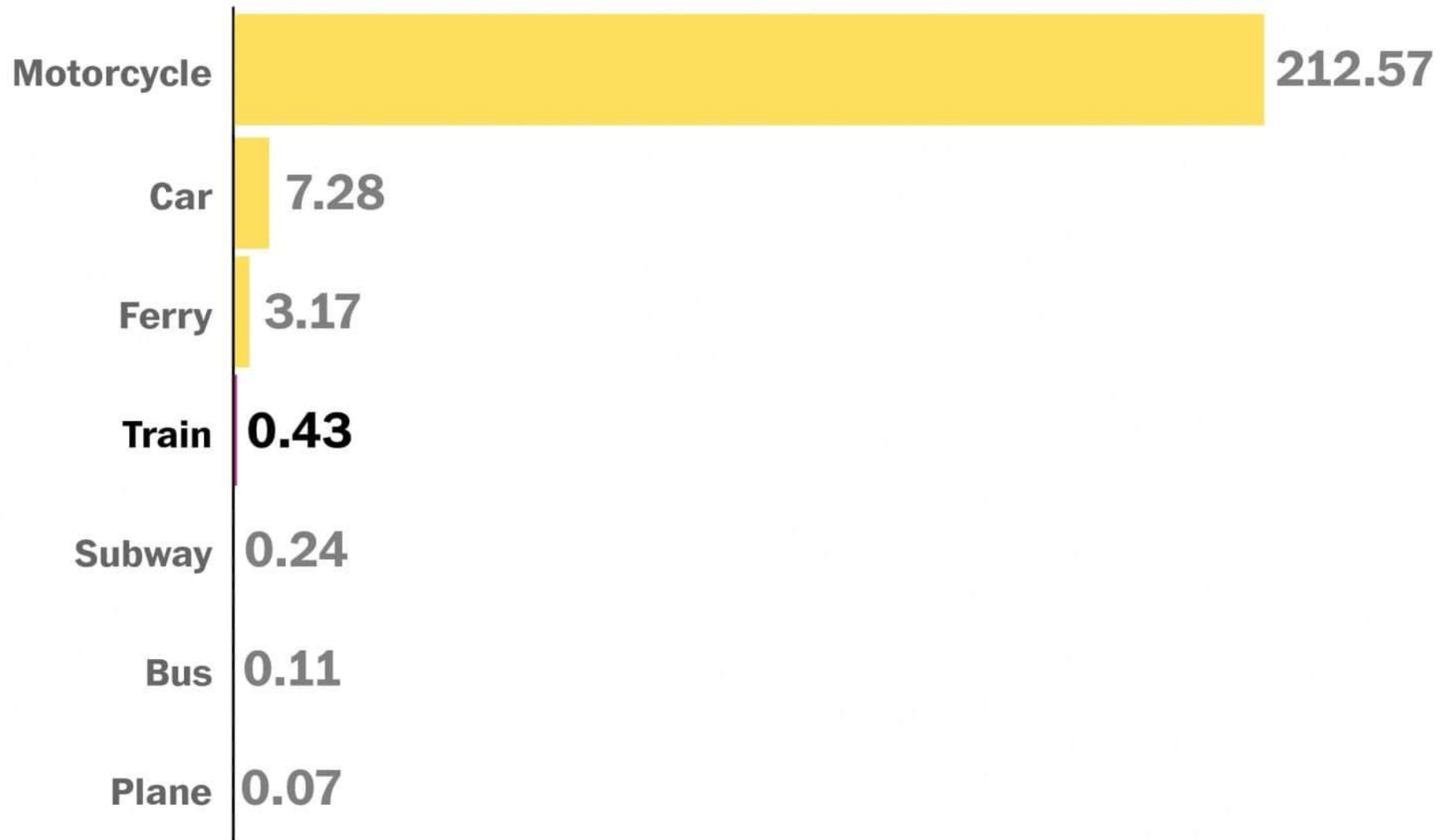
# HOW LONG DOES IT TAKE TO SCREW 12 SCREWS?

- Get your tools right.
- Get your own safety right.
- Being controlled by your buddy;
- Screw 12 screws;
- Being controlled by your buddy;
- Being controlled by the certification body;
- → 8h



# Motorcycles are the deadliest.

Passenger deaths per 1 billion passenger miles, 2000 to 2009



## Basic CIS Controls

- |   |   |   |  |
|---|---|---|--|
| 1 | Inventory and Control of Hardware Assets  | 2 | Inventory and Control of Software Assets           |
| 3 | Continuous Vulnerability Management   | 4 | Controlled Use of Administrative Privileges        |
| 5 | Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers | 6 | Maintenance, Monitoring and Analysis of Audit Logs |

## Foundational CIS Controls

- |    |   |    |   |
|----|---|----|---|
| 7  | Email and Web Browser Protections   | 8  | Malware Defenses                            |
| 9  | Limitation and Control of Network Ports, Protocols and Services                   | 10 | Data Recovery Capabilities                  |
| 11 | Secure Configuration for Network Devices, such as Firewalls, Routers and Switches | 12 | Boundary Defense                            |
| 13 | Data Protection   | 14 | Controlled Access Based on the Need to Know |
| 15 | Wireless Access Control   | 16 | Account Monitoring and Control              |

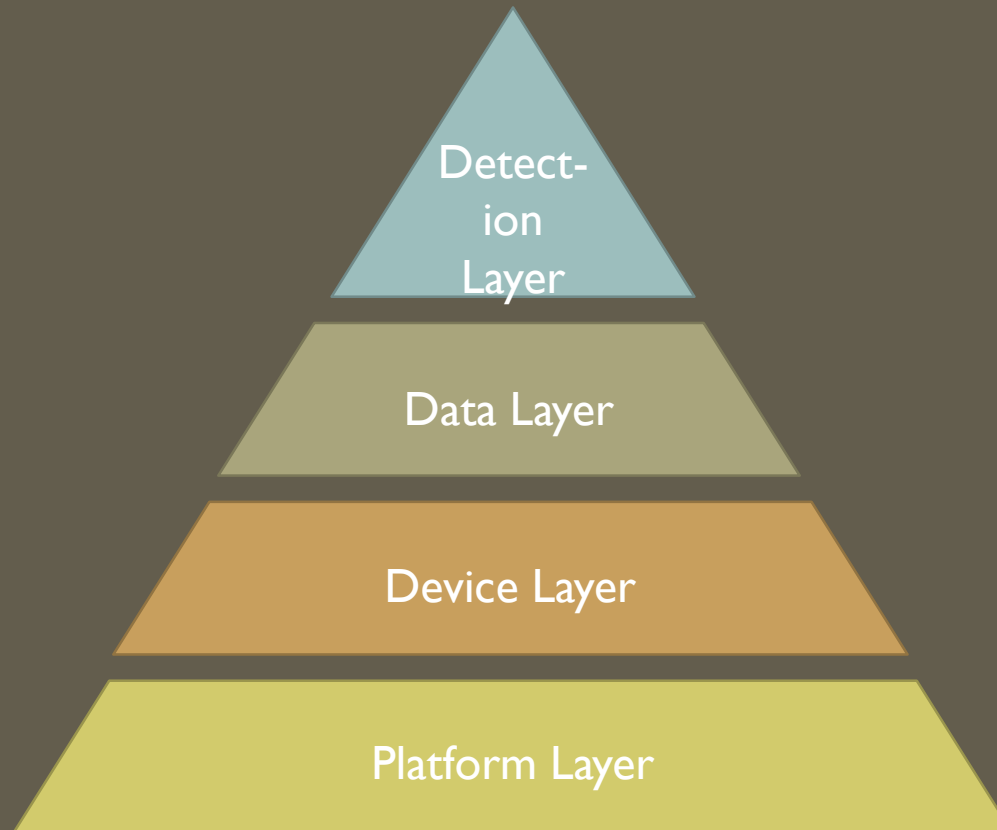
## Organizational CIS Controls

- |    |   |    |  |
|----|---|----|--|
| 17 | Implement a Security Awareness and Training Program | 18 | Application Software Security            |
| 19 | Incident Response and Management                    | 20 | Penetration Tests and Red Team Exercises |

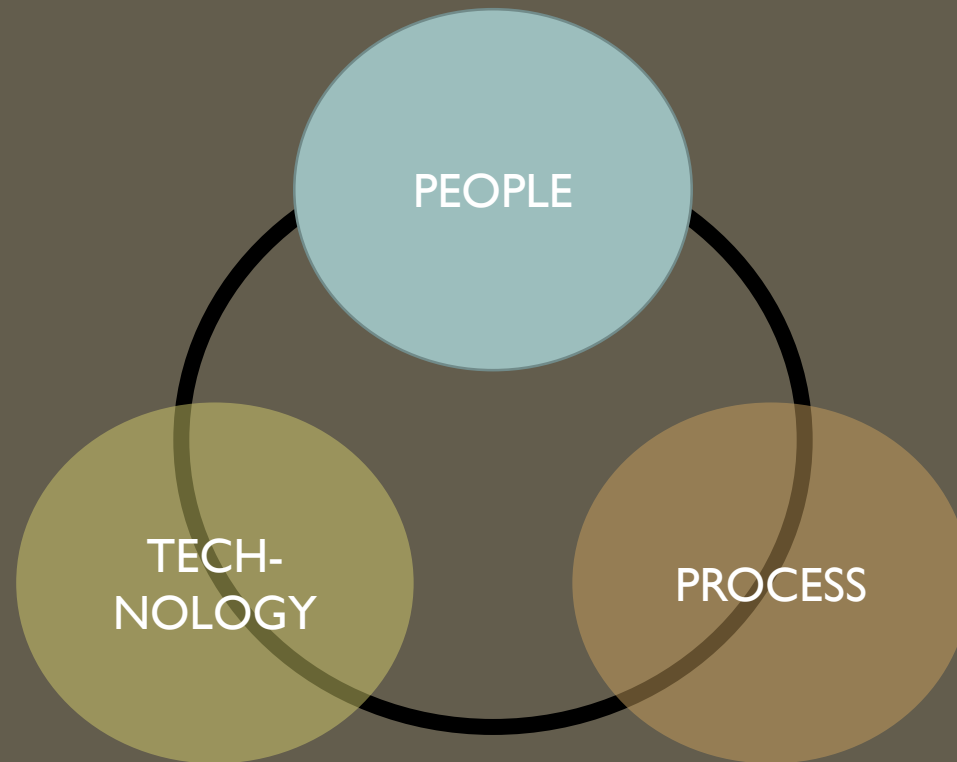
**SO GUYS WE DID IT**

**REACHED CIS CONTROL #6**

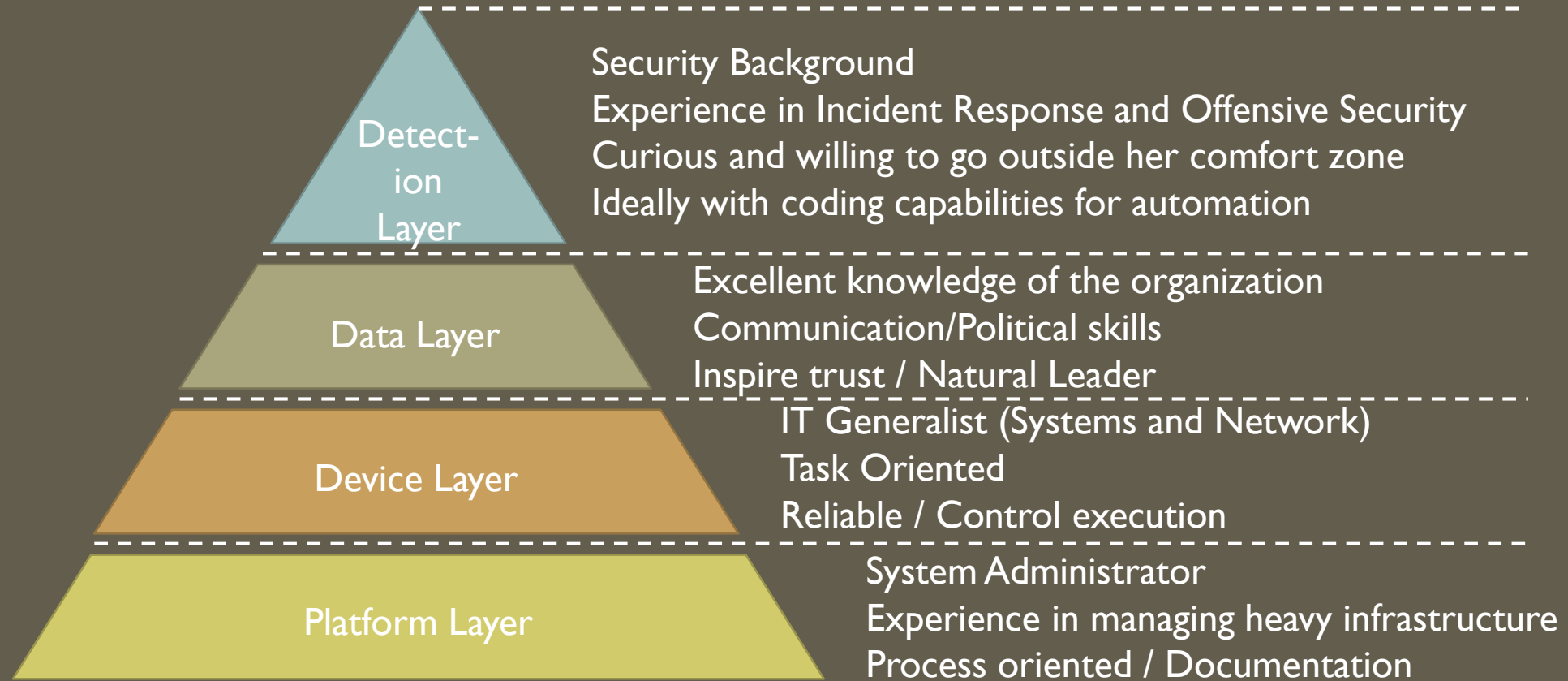
# PYRAMID OF JOY



# PEOPLE, PROCESS, TECHNOLOGY



# PEOPLE PROFILE





# PEOPLE

## 2 Staffs

Detection Layer	Security Analyst
Data Layer	
Device Layer	System Administrator
Platform Layer	

## 3 Staffs

Detection Layer	Security Analyst
Data Layer	Data Manager
Device Layer	System Administrator
Platform Layer	

## 4 Staffs

Detection Layer	2 x Security Analyst
Data Layer	Data Manager
Device Layer	System Administrator
Platform Layer	

## 5 Staffs

Detection Layer	2 x Security Analyst
Data Layer	Data Manager
Device Layer	Device Manager
Platform Layer	System Administrator

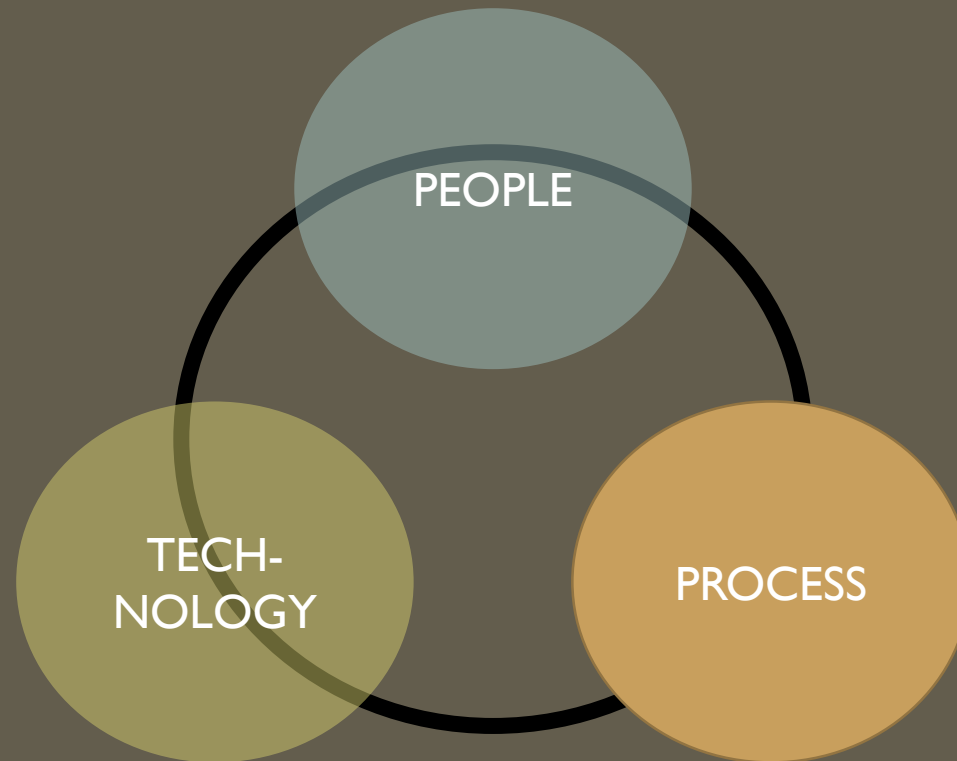
## 6 Staffs

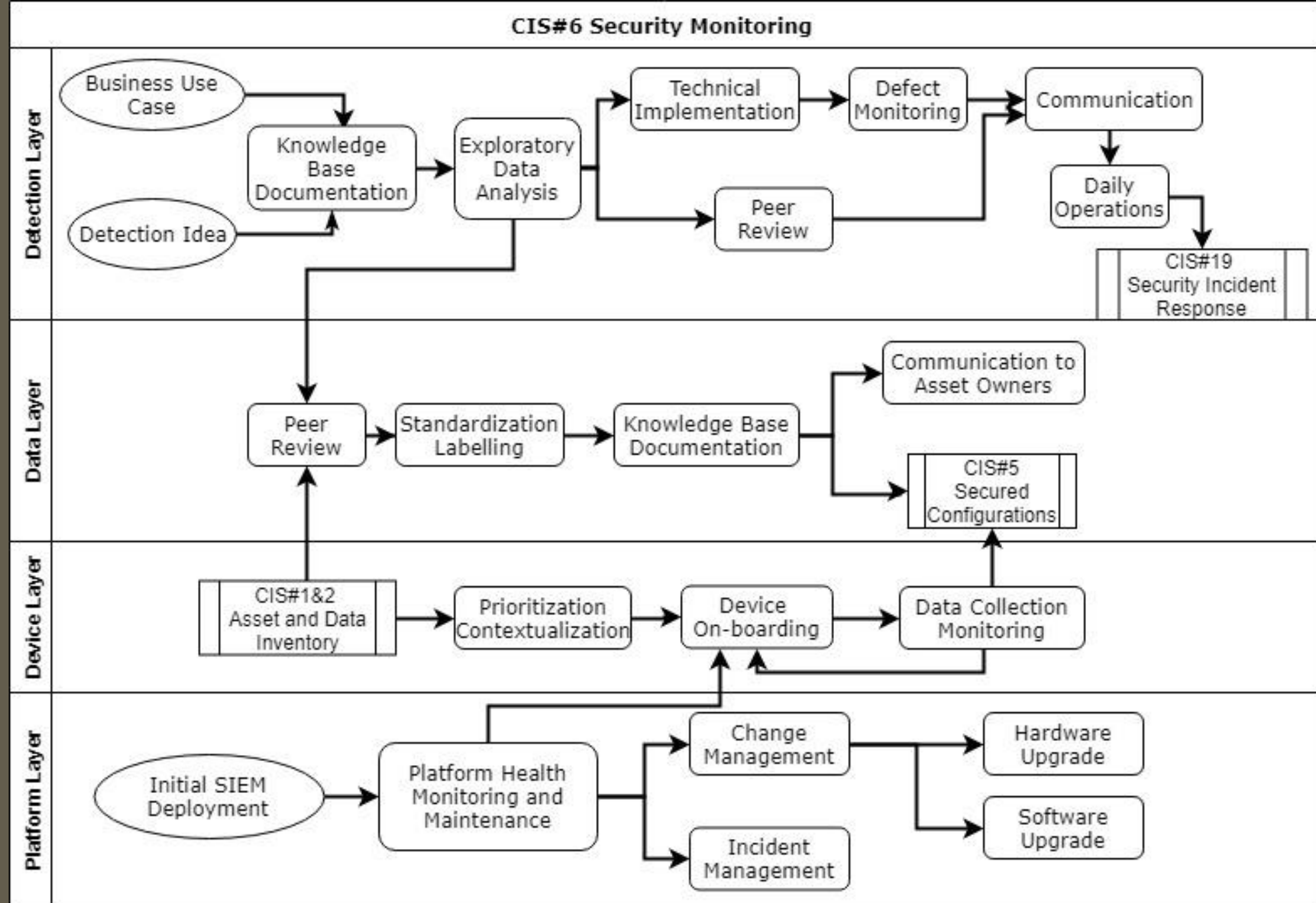
Detection Layer	3 x Security Analyst
Data Layer	Data Manager
Device Layer	Device Manager
Platform Layer	System Administrator

## 7 Staffs

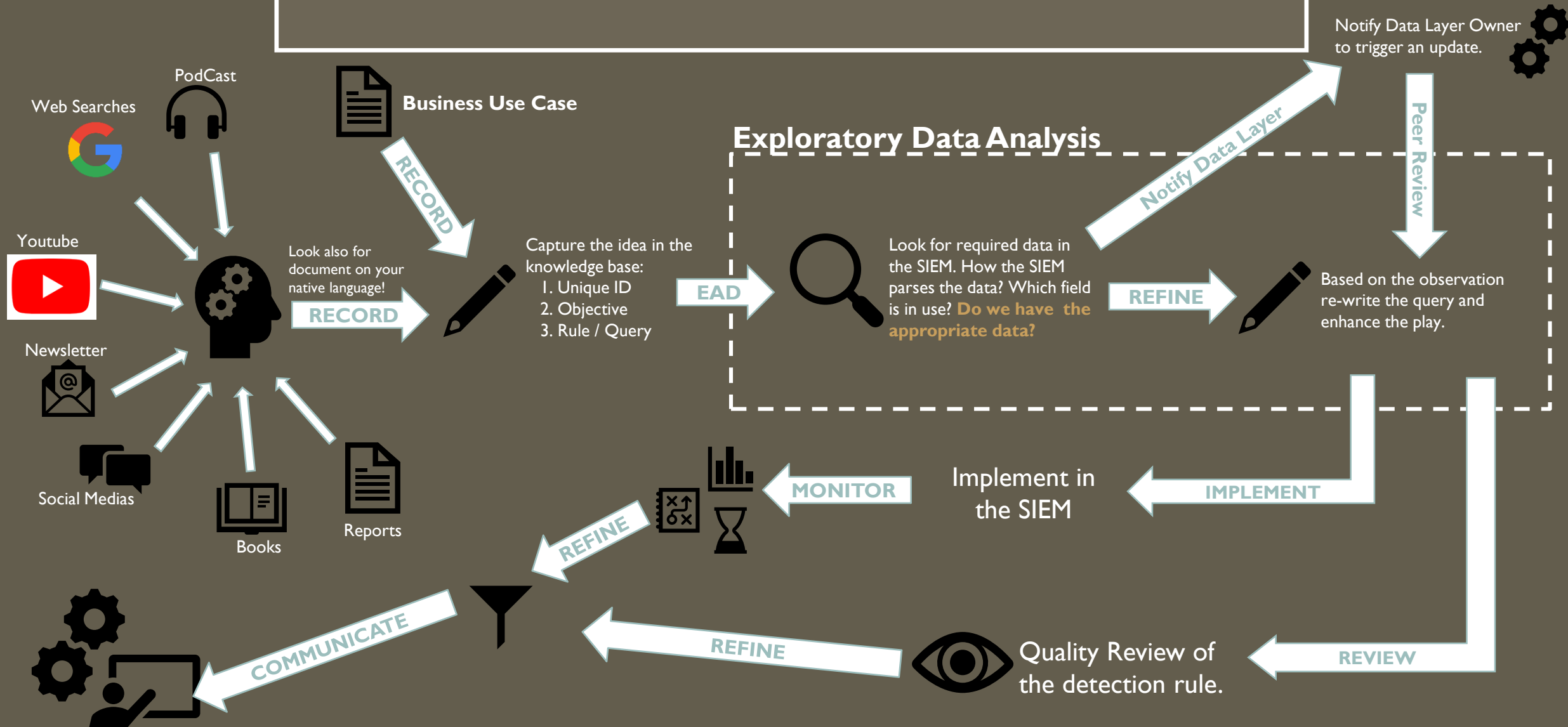
Detection Layer	3 x Security Analyst
Data Layer	Data Manager
Device Layer	Device Manager
Platform Layer	2 x System Administrator

# PEOPLE, PROCESS, TECHNOLOGY

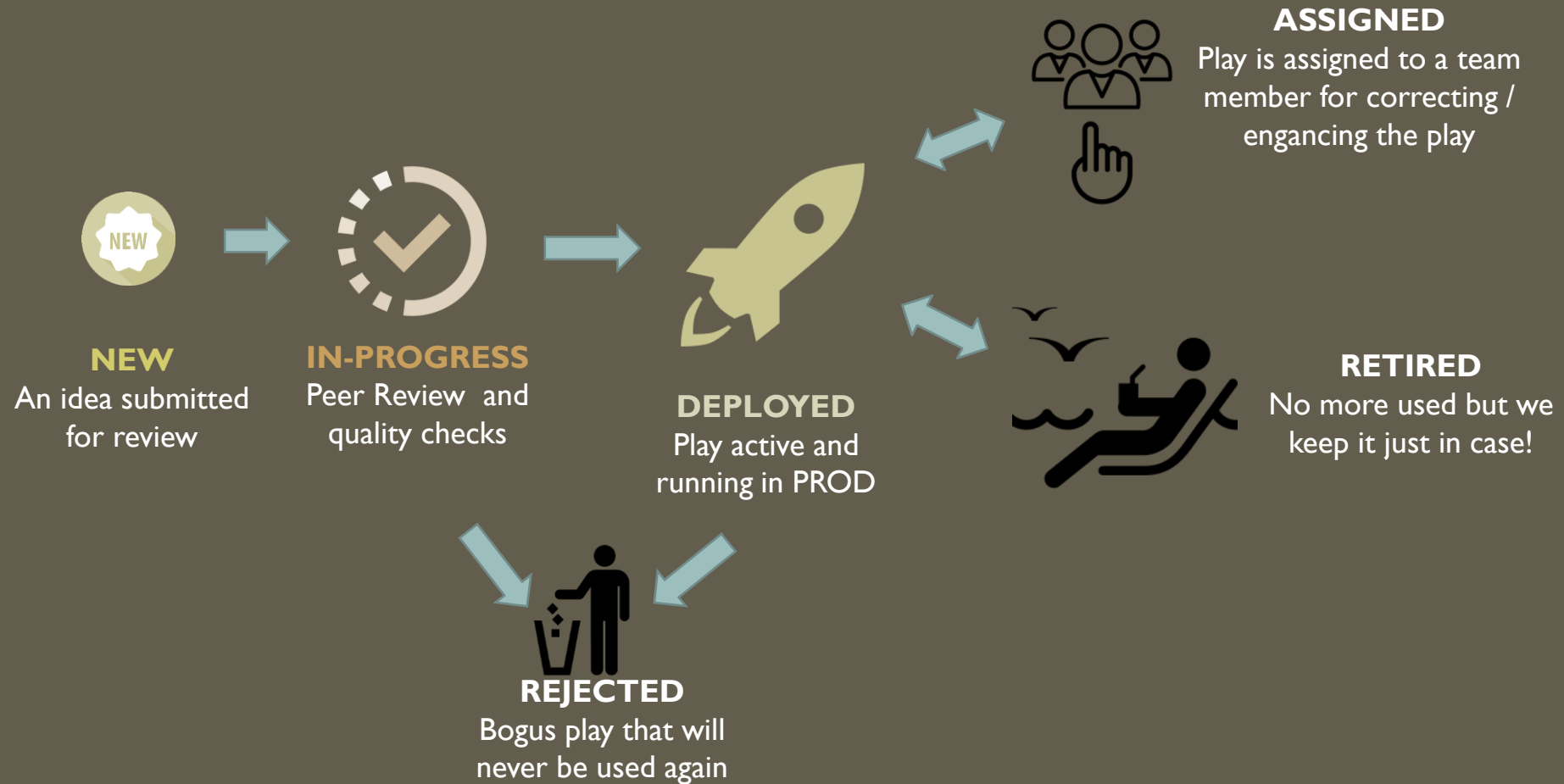




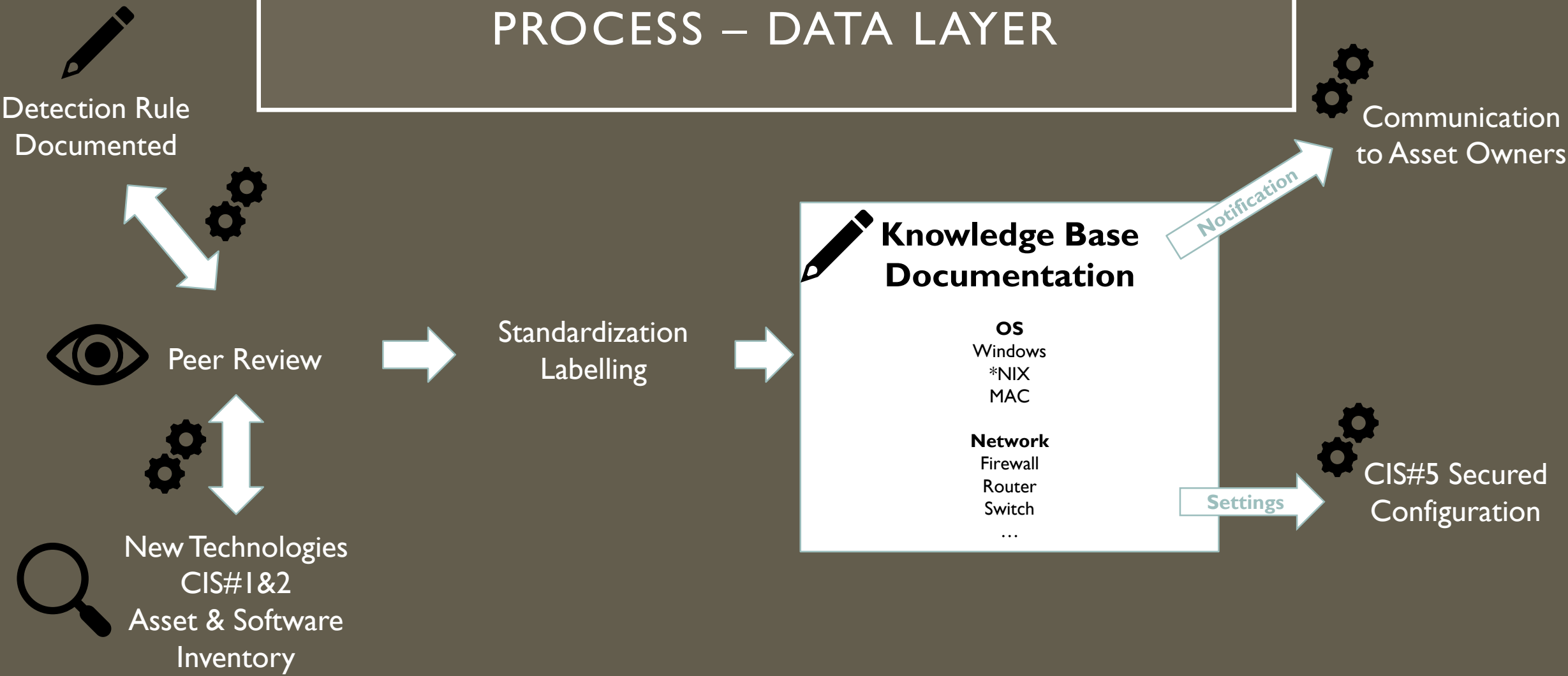
# PROCESS- DETECTION LAYER



## PROCESS - DETECTION LAYER



# PROCESS – DATA LAYER



# PROCESS – DEVICE LAYER

Data Layer



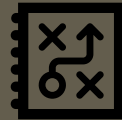
## CIS#1&2 Identify your Devices



CIS#1&2  
Asset & Software  
Inventory

Regularly scan for  
Asset Discovery

Identify



Prioritize your  
Assets

Onboard Device



Device  
On/Offboarding



Platform  
Monitoring

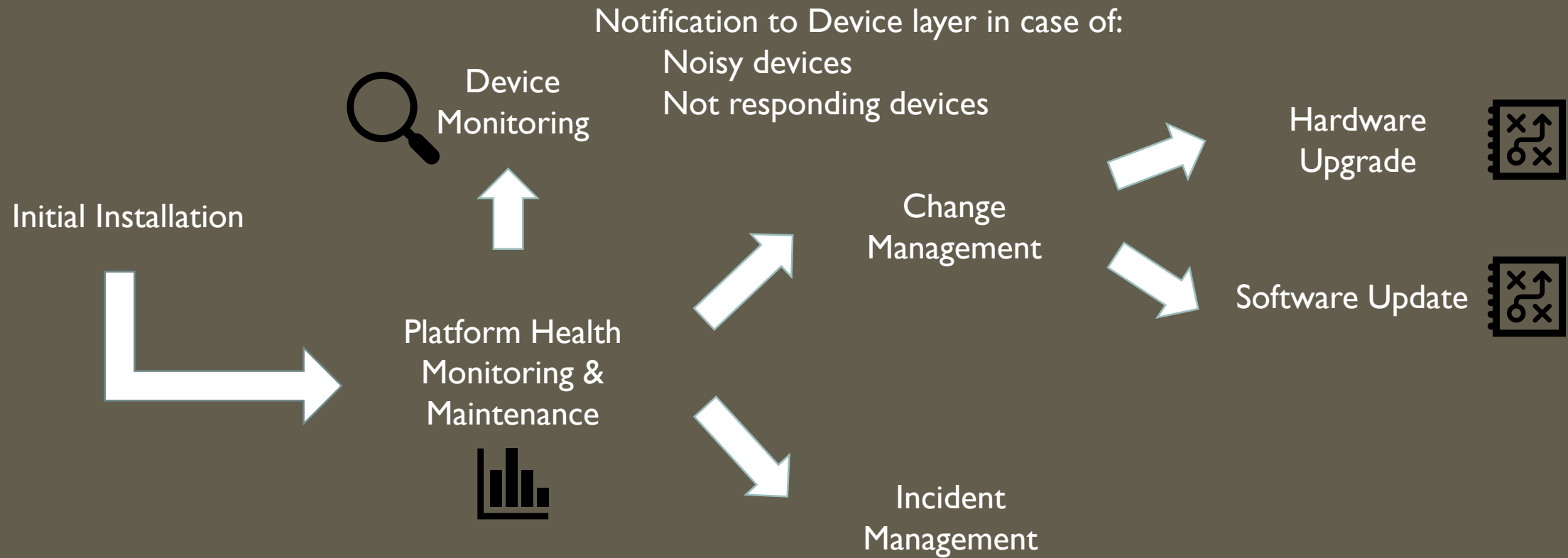


Data  
Collection  
Monitoring

CIS#5 Secured  
Configuration

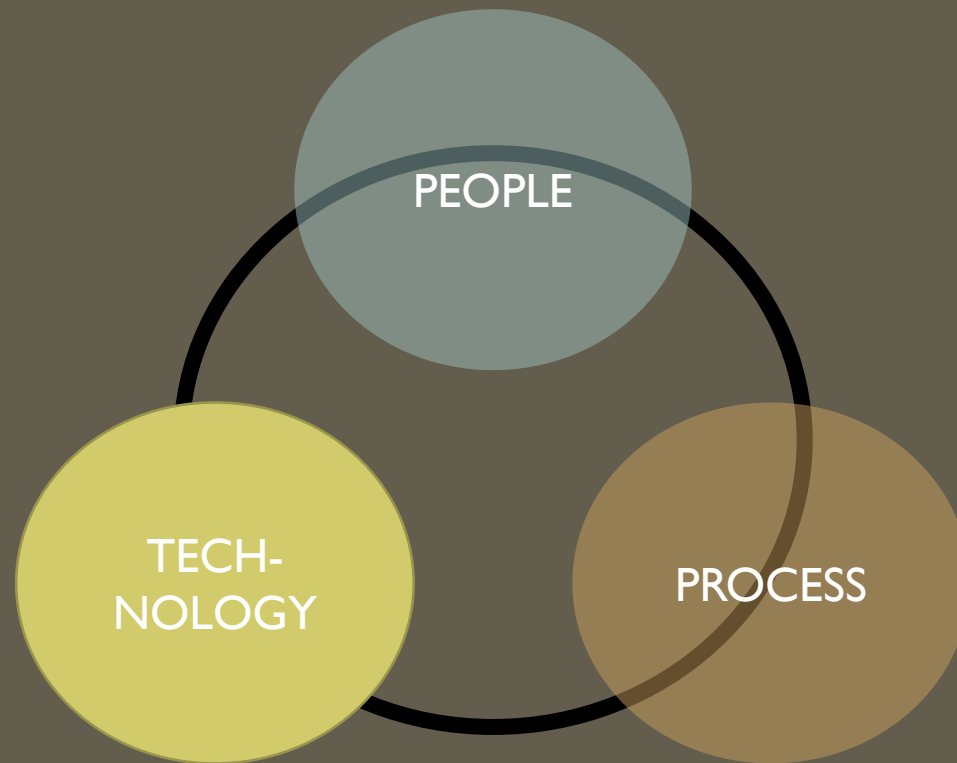


# PROCESS – PLATFORM LAYER





# PEOPLE, PROCESS, TECHNOLOGY



# TECHNOLOGY

SENSORS



Threat Intelligence feeds for enrichment



Enrichment

Event/Logs Parsers And Correlation Engine  
**graylog**

Ticketing System

Presentation System

Case Management

## FINAL THOUGHT

- Like far too many Infosec projects,  
Most security issues are first a  
people and process problem.  
Technology is a distant third;

QUESTIONS | COMMENTS | ABUSE



@Mag1cM0n