

# Beyond the Scan: The Value Proposition of Vulnerability Assessment

Damon J. Small, MSc.IA, CISSP  
Managing Consultant, IOActive

August 6, 2015



# About @damonsma11

- Managing Consultant at IOActive
- Louisiana native  
“Not from Texas but I got here as fast as I could!”
- In IT since 1995; infosec since 2001
- Spent much of my career supporting healthcare organizations in the Texas Medical Center
- Studied music at LSU; grad school in 2005 for Information Assurance
- Currently supporting a large oil & gas client in Houston

# Contact

## Email

[damon.small@ioactive.com](mailto:damon.small@ioactive.com)

[chef@securitykitchen.website](mailto:chef@securitykitchen.website)

[damon@damonsmall.me](mailto:damon@damonsmall.me)

## Blogs

[blog.securitykitchen.website](http://blog.securitykitchen.website)

[ramble.damonsmall.me](http://ramble.damonsmall.me)



[@damonsmall](https://twitter.com/damonsmall)

More than just clicking “scan...”

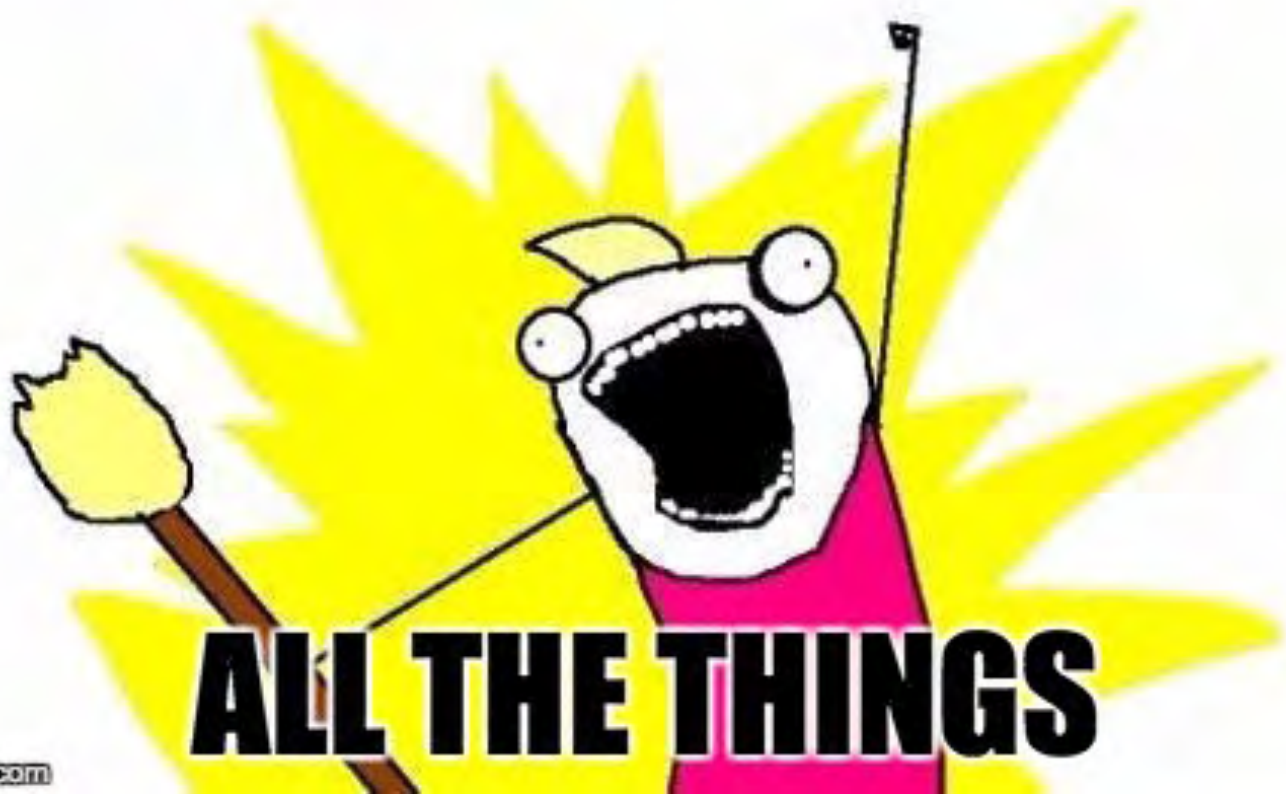
[#BlueCollarSecurity](#)

Red Team



Blue Team

**SCAN**



**ALL THE THINGS**

**Scan  
Data**

**Actionable  
Information**

**Human  
Analysis**

**RAPID7**  
nexpose®

 **QUALYS®**

**SAINT®**

 **Nessus**  
Network Vulnerability Scanner

# Overview

1. Identifies potential vulnerabilities
2. Provides remediation information
3. Asset Management\*
4. Software Management\*
5. Compliance
6. Strategic – on-going operational intelligence
7. Tactical – Incident Response

\*Not generally a named feature, but a result of the activity.



# But first, a history lesson

- Security Administrator Tool for Analyzing Networks (SATAN)
- Released in 1995 and polarized the security industry

PC Mag, April 23, 1996



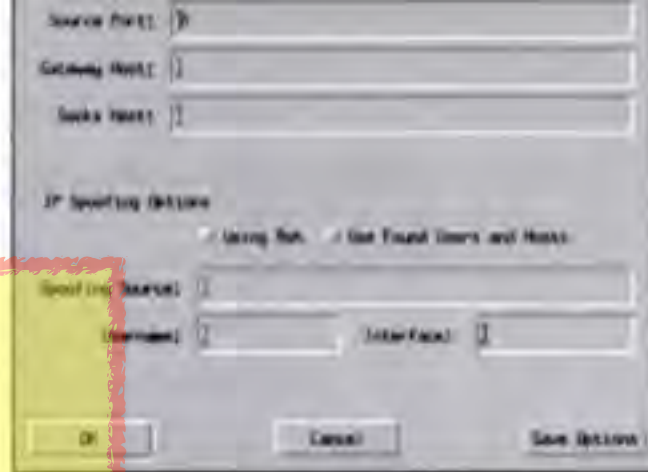
“The [DOJ] became concerned... and threatened to press charges against... Dan Farmer....”

“...Internet Scanner can check for more than 100 known vulnerabilities.”

for lapses in security. The first of the network scanners, Security Administrator Tool for Analyzing Networks (**SATAN**), gained notoriety in the summer of 1995.

The United States Justice Department became concerned about national security issues raised by **SATAN** and threatened to press charges against Silicon Graphics where **SATAN**'s coauthor, Dan Farmer, worked. But Farmer was fired, the Justice Department dropped its investigation, and development of these devices goes on.

Though Internet Scanner has maintained a lower profile than **SATAN**, it is much easier to use than **SATAN** or Qualix Group's NetProbe, another direct competitor. And Internet Scanner scans for a more ex-



fact, Internet Scanner can check for more than 100 known vulnerabilities. After the scans are run, Internet Scanner generates HTML-based reports, giving administrators road maps to where security might be breached on their networks.

Internet Scanner can also check for *spoofing*, a popular method of gaining access to a network through its firewall by which an unauthorized host emulates an authorized one.

To test, we installed the product on a Windows 9.03. The IBM AIX versions of the software are in the process of being released.

The application is compressed and we installed it on our test system. Our test system has a firewall, which we used to test Sun SP.

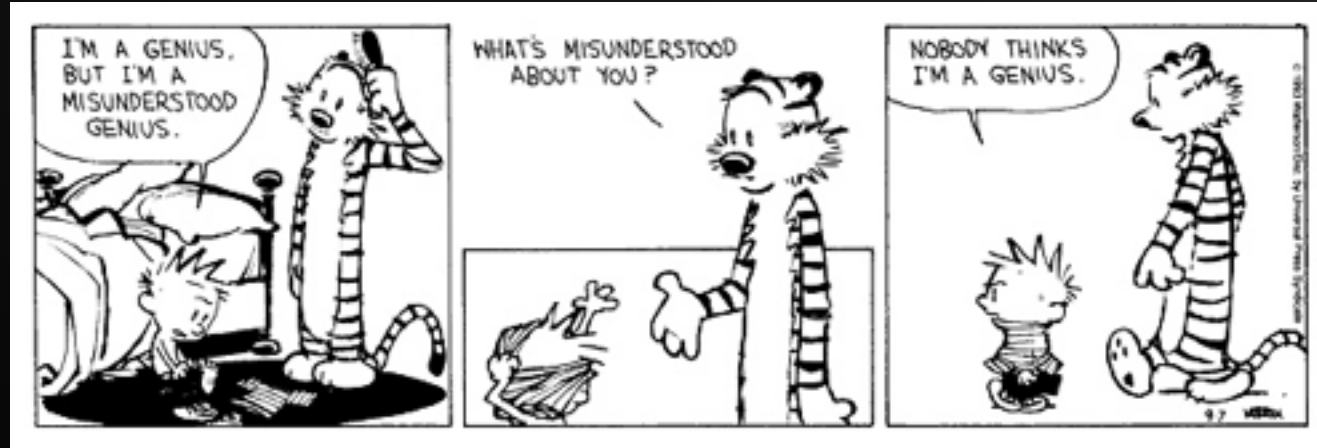
# Where are they now?

- [http://en.wikipedia.org/wiki/Dan\\_Farmer](http://en.wikipedia.org/wiki/Dan_Farmer)
- [http://en.wikipedia.org/wiki/Wietse\\_Venema](http://en.wikipedia.org/wiki/Wietse_Venema)
  
- Richard Carson & Donna Ruginski forked Security Administrator's Integrated Network Tool (SAINT) from SATAN in 1995
- SAINT Became a commercial product in 1998

# From those humble beginnings...

- An entire new capability was created for infosec
- Progression from
  - Simple scanning
  - Vulnerability Assessment
  - Vulnerability Management

**Scanners have been around for two decades....**



...but are still misunderstood.

What is being examined  
What tool can be used

User-facing web app  
Web Inspect, Burp

Thick-client apps  
IDA Pro, Sys Internals

TCP/UDP/IP, ports  
nmap

Electrons/Photons going through wire/fiber

# OSI Model

Host Layers

7. Application

6. Presentation

5. Session

4. Transport

Media Layers

3. Network

2. Datalink

1. Physical

The entire stack  
Manual, human-based testing

Network, software, & OS info  
Nexpose, Qualys, Nessus,  
SAINT

TCP/IP, ports, protocols, MAC  
Wireshark, tcpdump, windump



## Tools

Network, software, & OS information  
Nexpose, Qualys, Nessus, SAINT

## Automated Scanners

- Large number of hosts
- Integration of data to other systems

### Limits:

- Software information is basic
- “Dumb”
- Unaware of business logic flaws

# OSI Model

7. Application

5. Session

4. Transport

3. Network

2. Datalink

1. Physical

Host

Media Layers

## People

The entire stack  
Manual, human-based testing

## Manual, Human-based Testing

- Validation of vulnerabilities
- Advanced configuration issues
- Memory analysis
- Vulnerability chaining
- Cannot be done with software

- Resource-intensive

*\*Although this seems straight-forward, it fills a methodology document that is hundreds of pages long.*

The tools are critical but their usefulness is limited without skilled security professionals

For example: HTTP vulnerability false positives?



# Define Your Lexicon

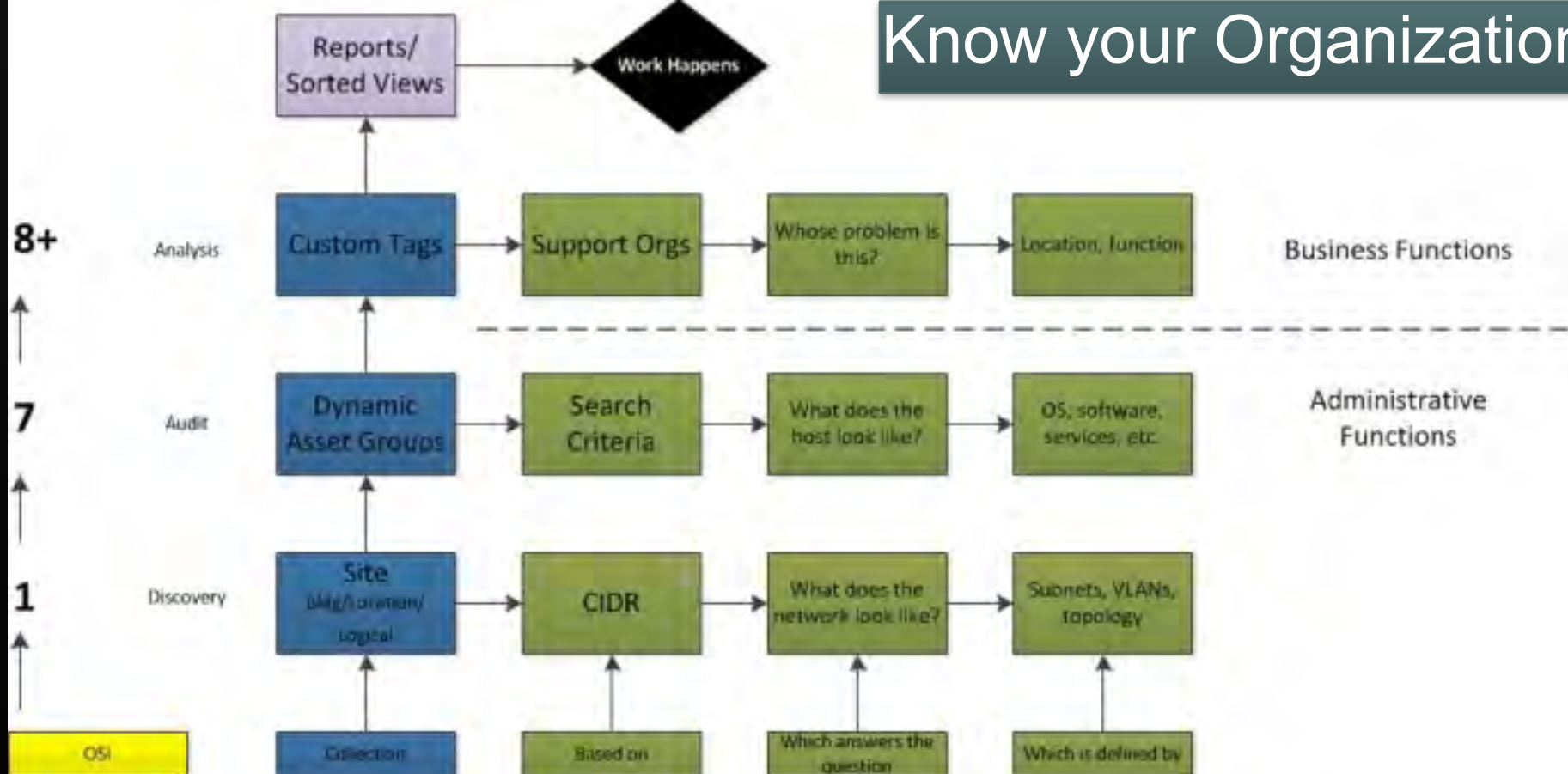
- Application - the 7th layer of the OSI Model.
- Application - software that a human uses.
  
- Interface - connects a host to a network (NIC).
- Interface - software that allows programs to share info.
- Interface - software that allows humans to interact with computers/apps.
  
- Session - the 5th layer of the OSI Model.
- Session - interaction between a browser and server.
  
- Server - hardware that runs a network OS.
- Server - software that responds to client requests.

# Know your Environment



What is the architecture of your network,  
both logically and physically?

# Know your Organization



**Critical Success Factor**

How will the data be consumed and acted upon?

# Case Studies



# 1. Identifies Potential Vulnerabilities

A target with concentric rings of blue, red, and yellow, with a dart hitting the center. The target is set against a dark background. The dart is positioned diagonally from the bottom right towards the center of the target.

“What are attractive targets?”

“What patches are missing?”

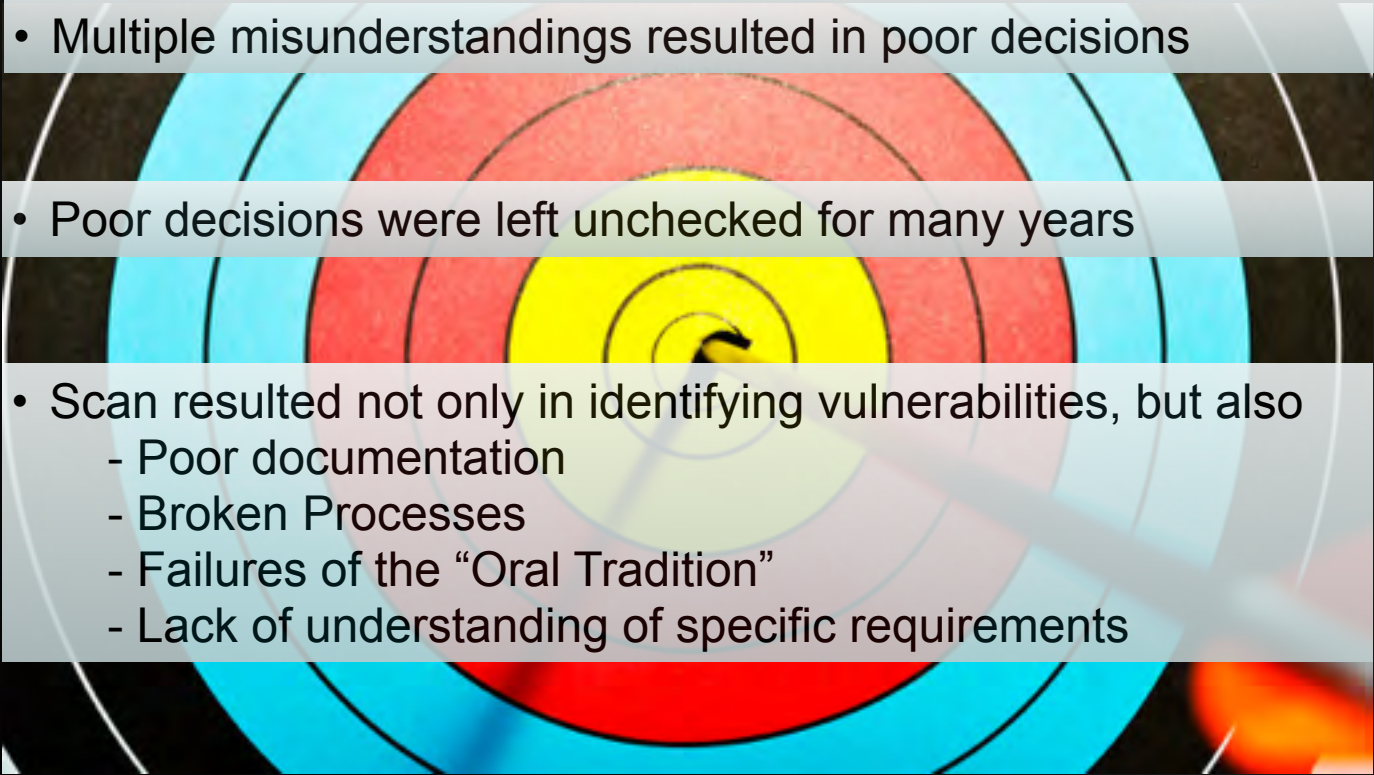
“Is our environment configured properly?”

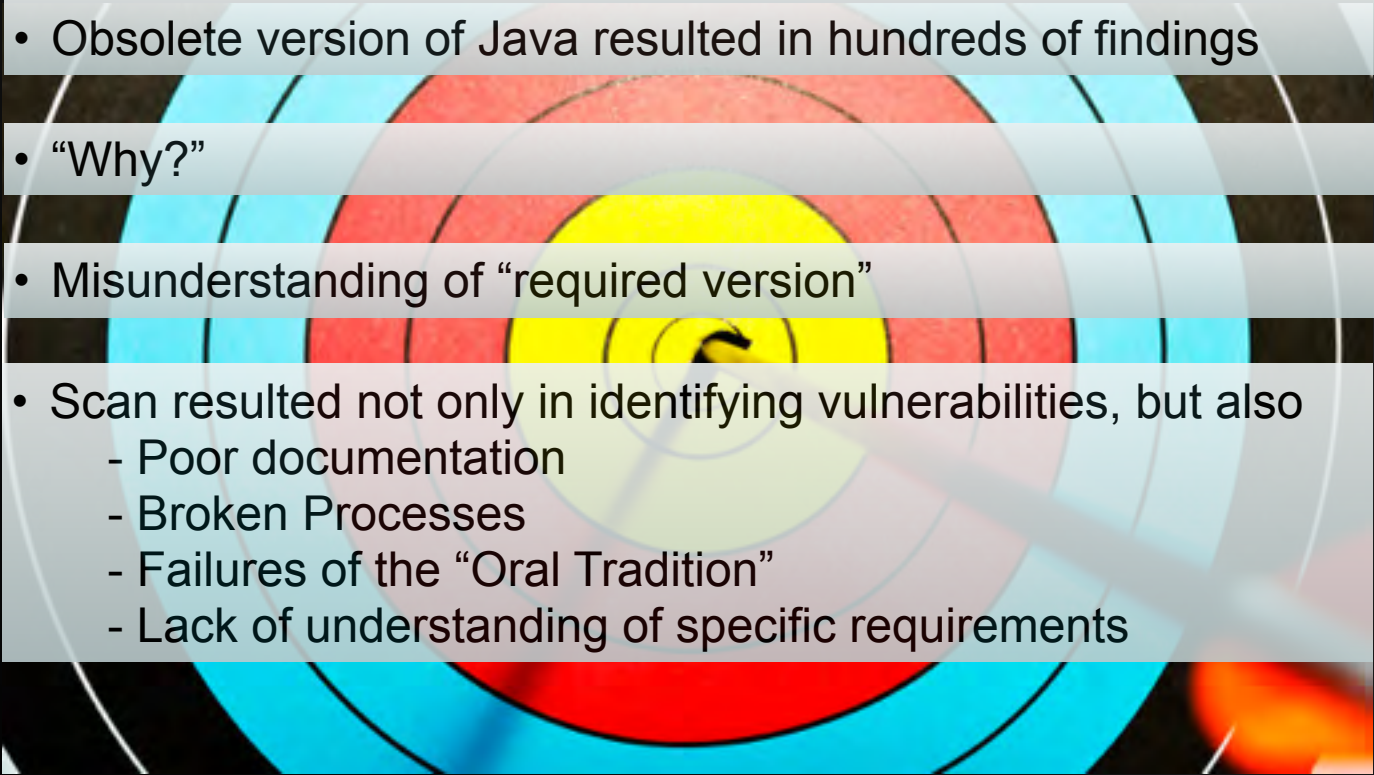


- Perimeter scan revealed CIFS
- Ports 135, 139, 445
- Hosts were largely Windows XP (late 2013)

- Assessment team asked “why?”
- Answer: “Necessary for support.”
- LPT: It is never a good idea to expose NetBIOS ports on a Windows machine to the Internet

- Legacy business app required IP-based authentication
- Static NAT assignments were made - each host had a routable IP Address
- Inbound rule was **any any accept**

- 
- Multiple misunderstandings resulted in poor decisions
  - Poor decisions were left unchecked for many years
  - Scan resulted not only in identifying vulnerabilities, but also
    - Poor documentation
    - Broken Processes
    - Failures of the “Oral Tradition”
    - Lack of understanding of specific requirements

- 
- Obsolete version of Java resulted in hundreds of findings
  - “Why?”
  - Misunderstanding of “required version”
  - Scan resulted not only in identifying vulnerabilities, but also
    - Poor documentation
    - Broken Processes
    - Failures of the “Oral Tradition”
    - Lack of understanding of specific requirements



## 2. Provides Remediation Information



# 3. Asset Management

- Scanning known hosts vs CIDR blocks

- Client discovered active “dark” network segments

- Client compares scan information with CMDB

- Anything with an IP Address - cameras / Nintendo

- Drilling company - platforms had “exactly 4 hosts per rig”

*“The kid’s good.”*



**Daniel Miessler**

@DanielMiessler



Following

Running an infosec program is 90% asset management. 90% meaning that if you're not doing it you're screwed no matter what else you're doing.



RETWEETS

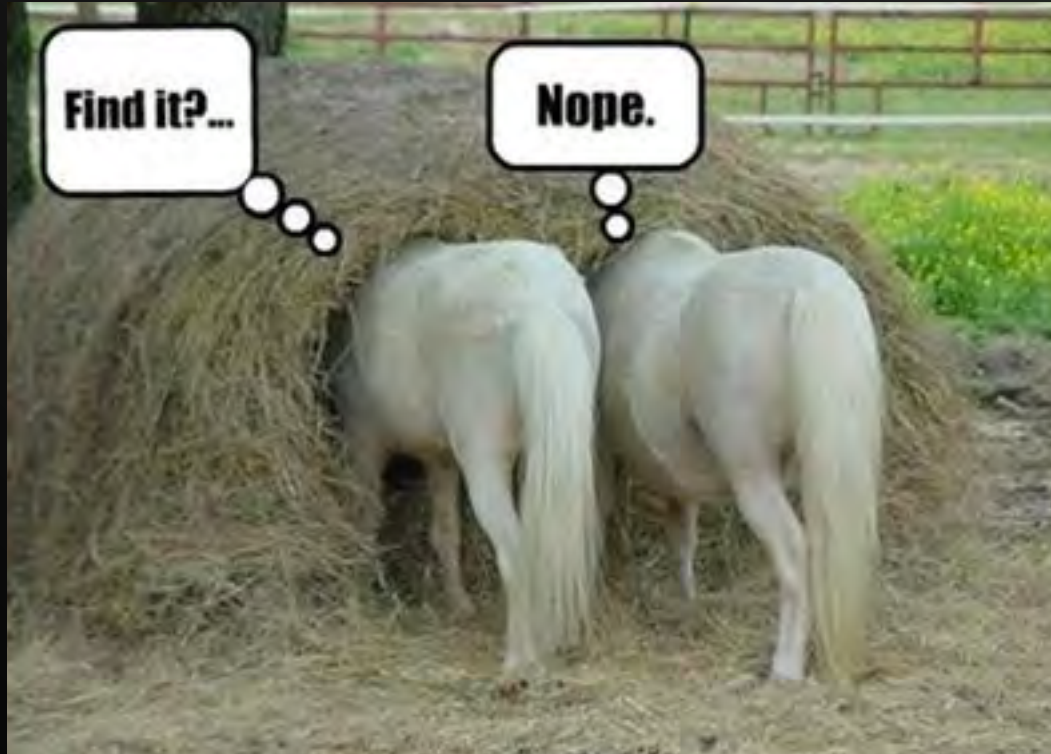
4

FAVORITES

5



## 4. Software Management



## 6. Compliance



# 7. Strategic Planning







# Biomedical/ICS





# Special Considerations: Biomedical Devices

- FDA 510(k) limits changes to devices once marketed
- <http://tinyurl.com/FDA510kblog>
  - Redirects to a post on <http://blog.securitykitchen.website>
- Security vs Supportability - not unique to healthcare but leads to poor design decisions
  - Radiology Reading Stations with FTP
  - Clinical protocols like HL7 are cleartext so compensating controls are necessary
  - How do you manage your HL7 interface engines?

# Special Considerations: Industrial Control Systems

- Operational Technology (OT) is not the same as Information Technology (IT)
- Shutting down ICS is costly - patch cycles are lengthy
- Not unusual to operate with malware present
- Purpose-built devices may not handle unexpected traffic with grace
- Be extremely cautious with active scanning; consider passive scanning

**In Conclusion...**

