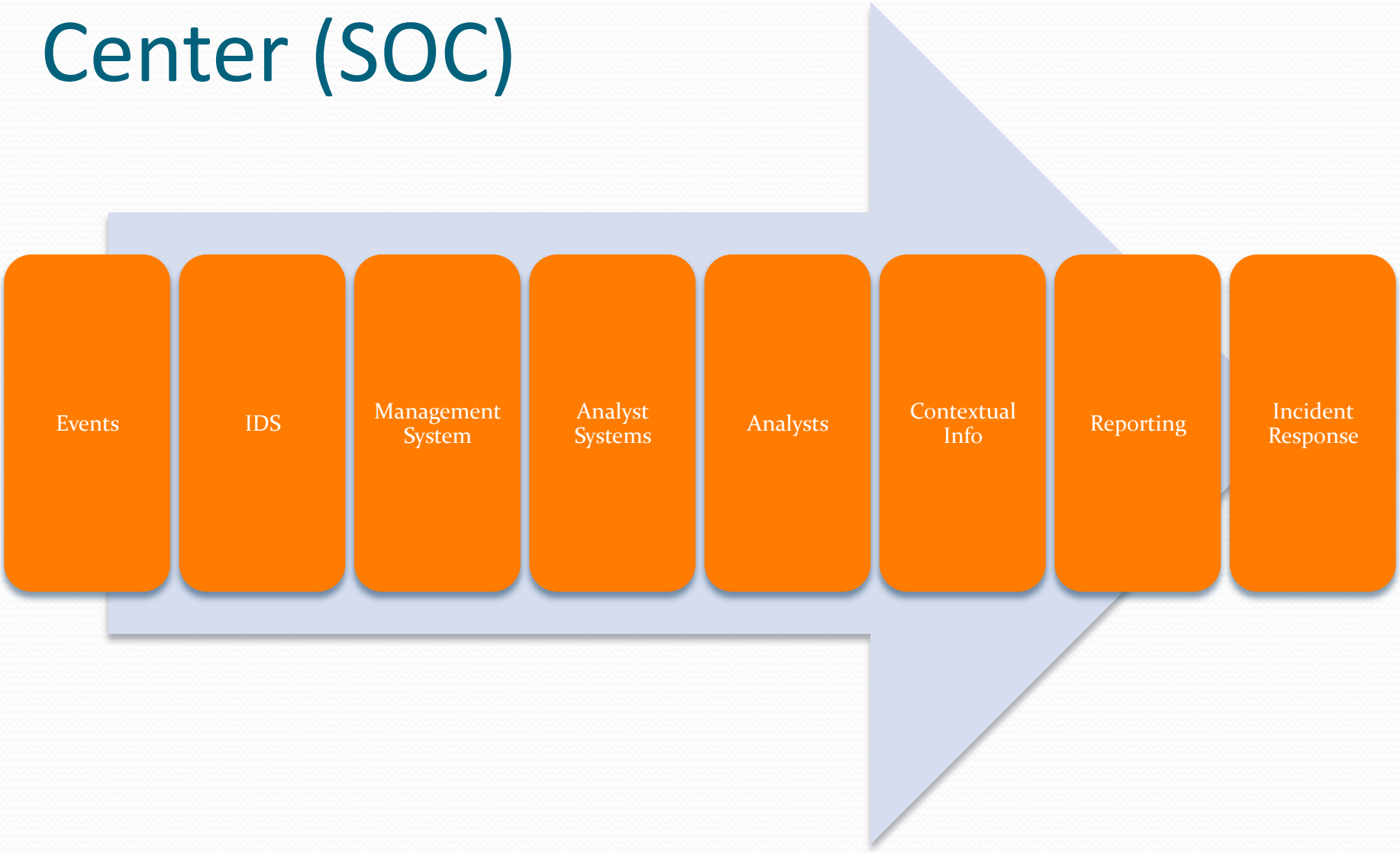
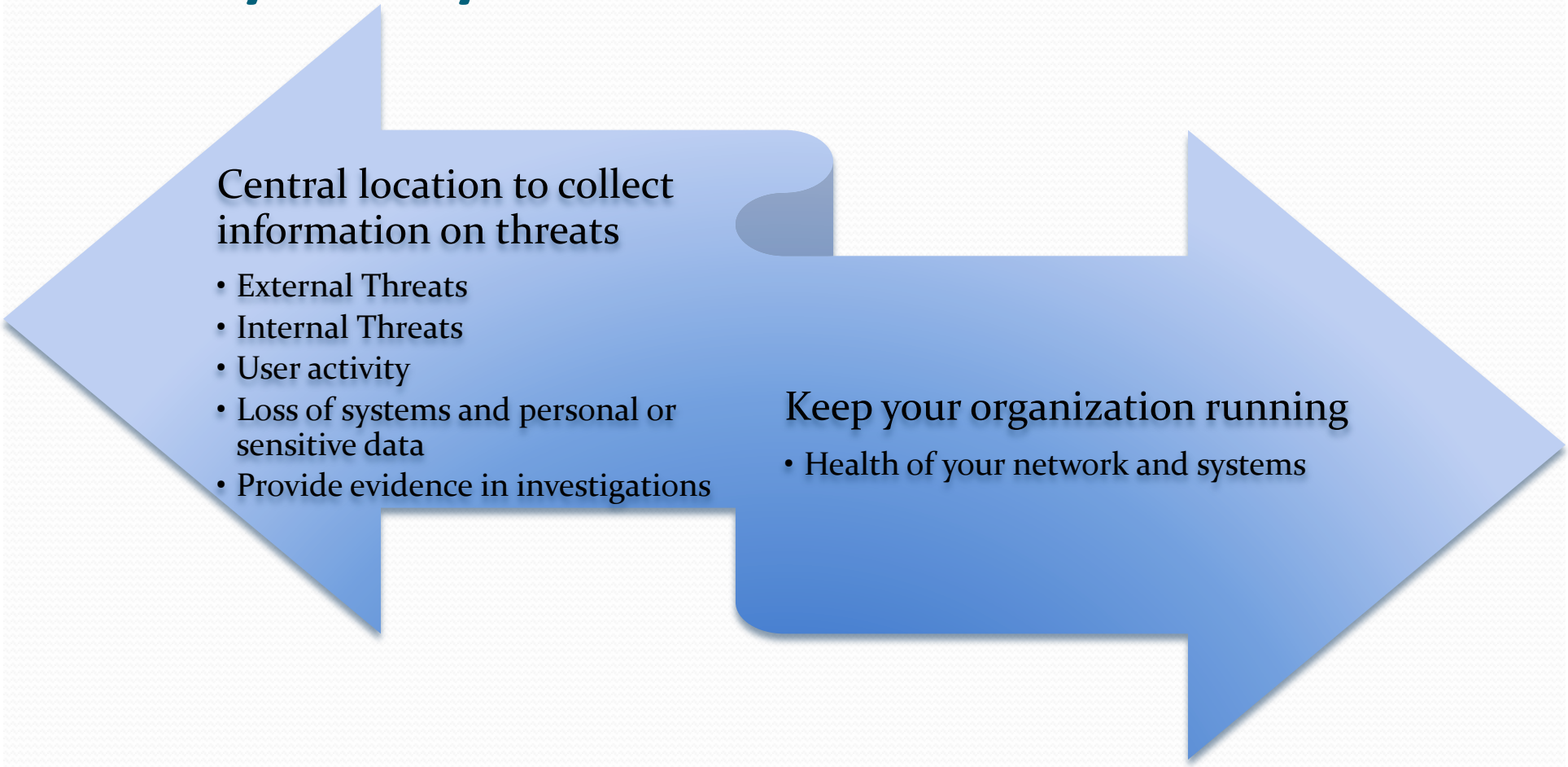
Building a Security Operations Center.

For little or no money…

What is a Security Operations Center (SOC)



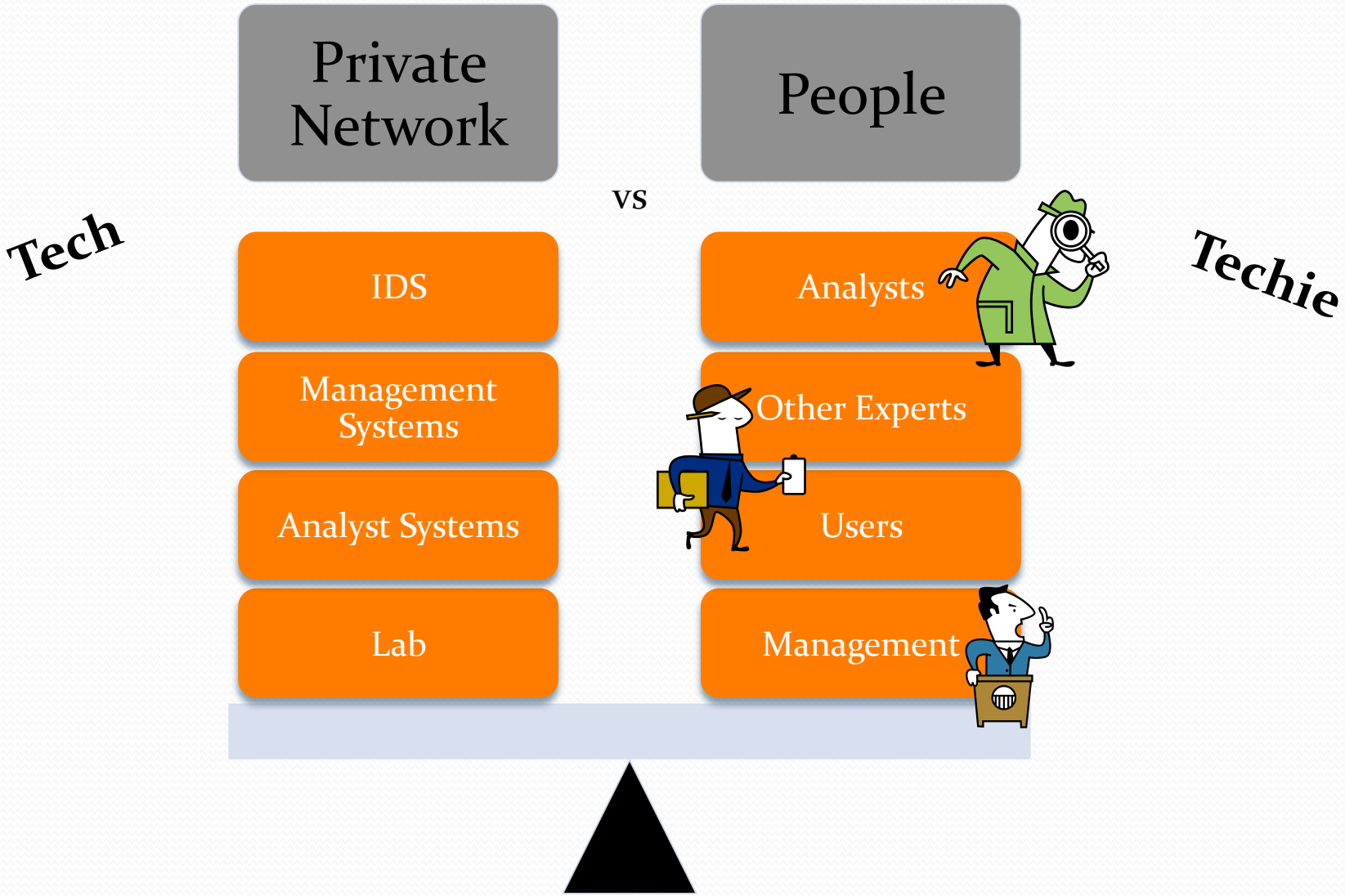
Why do you need a SOC?



Isn't a Firewall, IDS or AV enough?

- Firewall is active and known by attackers
  - Protects your systems, not your users
- Anti-Virus
  - Lag-time to catch new threats
  - Matches files, but not traffic patterns.
- IDS alerts on events, but doesn't provide context
  - System logs
  - Proxy logs
  - DNS logs
  - Information from other people

Structure of a SOC

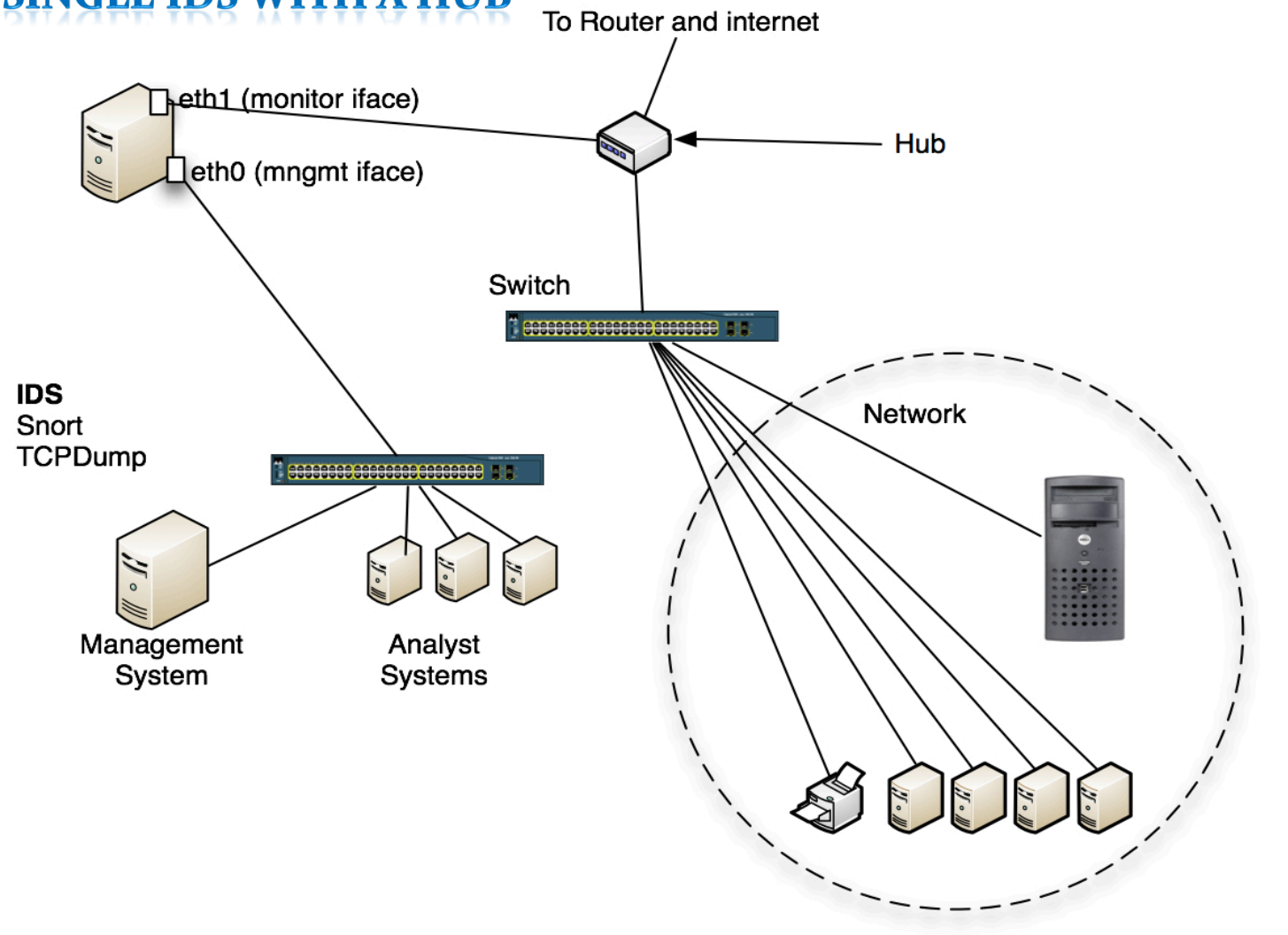


Techie using real-time tech 24/7

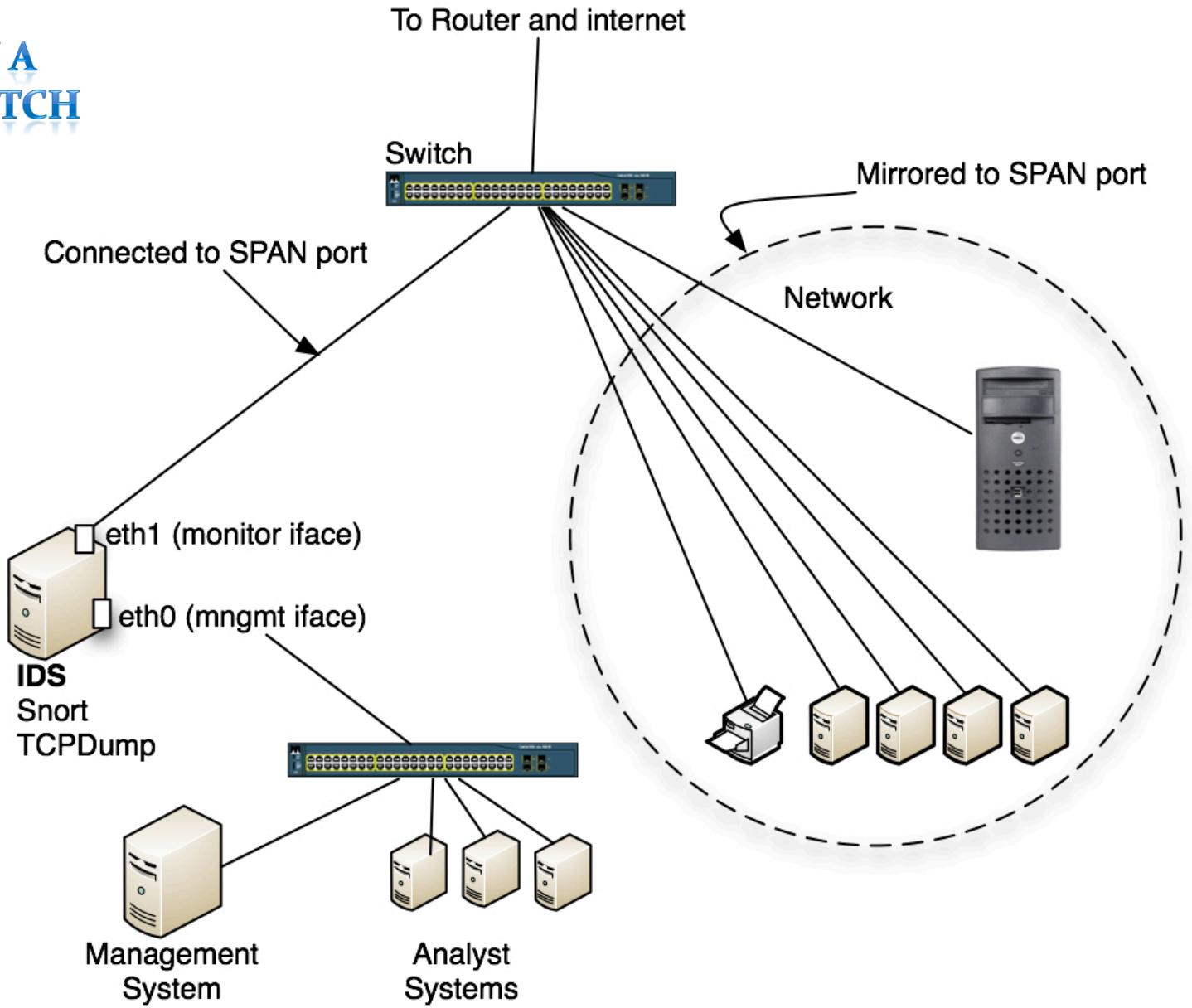
Private network

- Secure communication between
  - IDS
  - Management System
  - Analyst Systems
- Management and update of IDS and rules

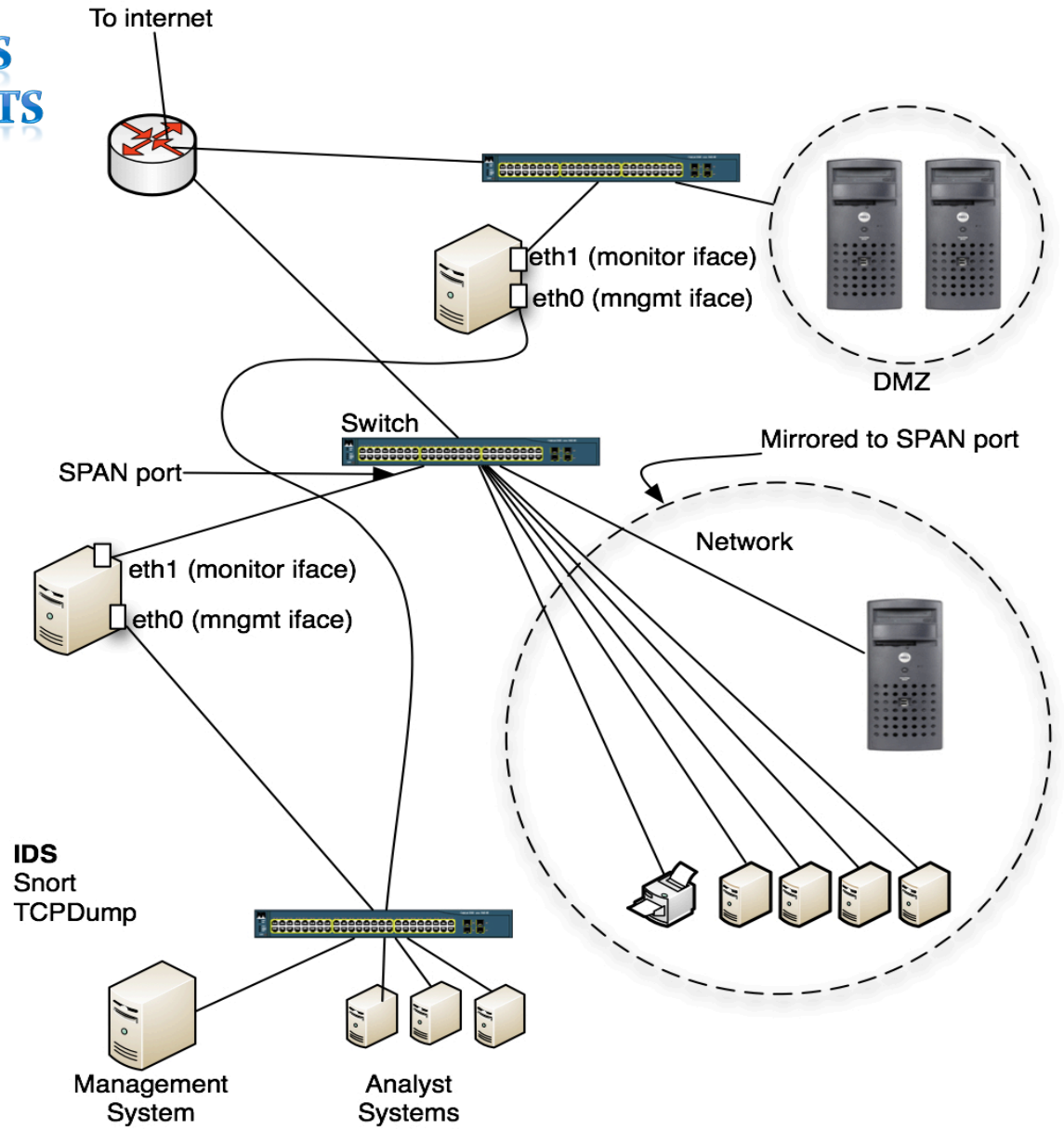
SINGLE IDS WITH A HUB



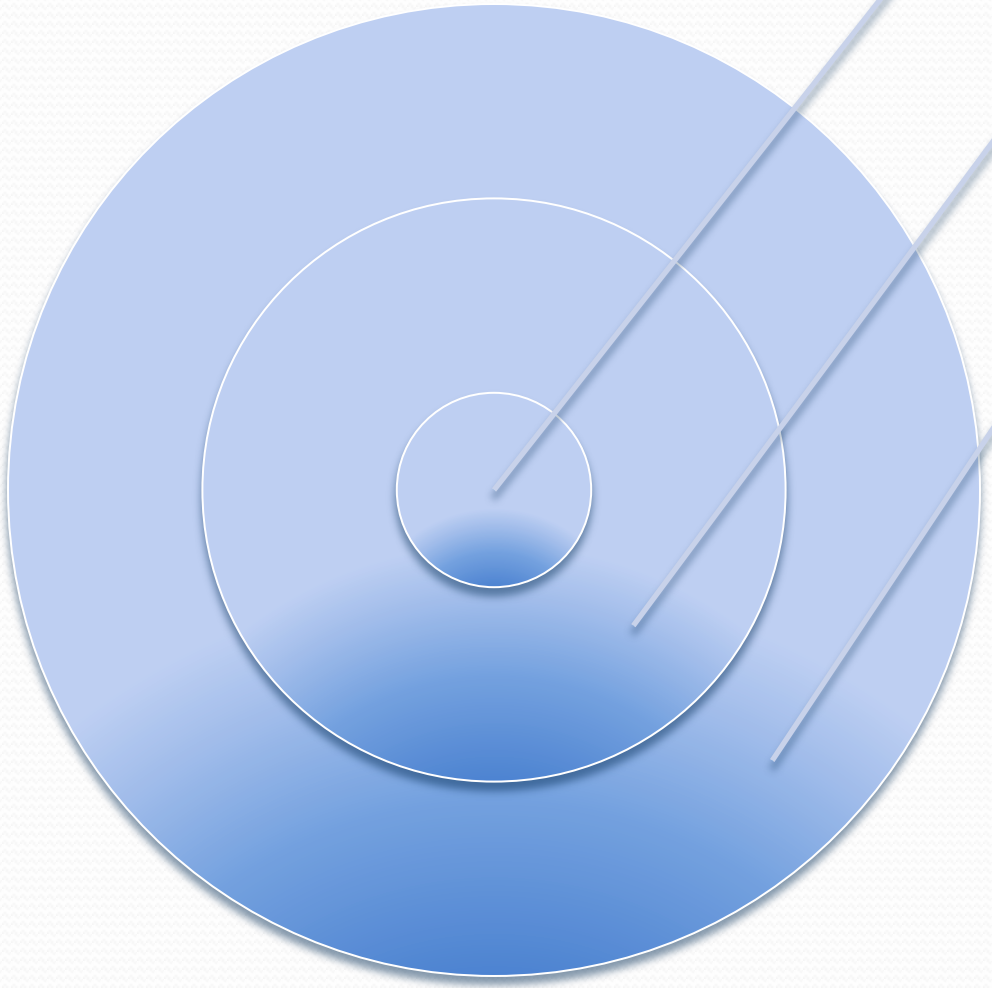
SINGLE IDS ON A MANAGED SWITCH



MULTIPLE IDS SYSTEMS TO MONITOR SEGMENTS



IDS system



Secured OS

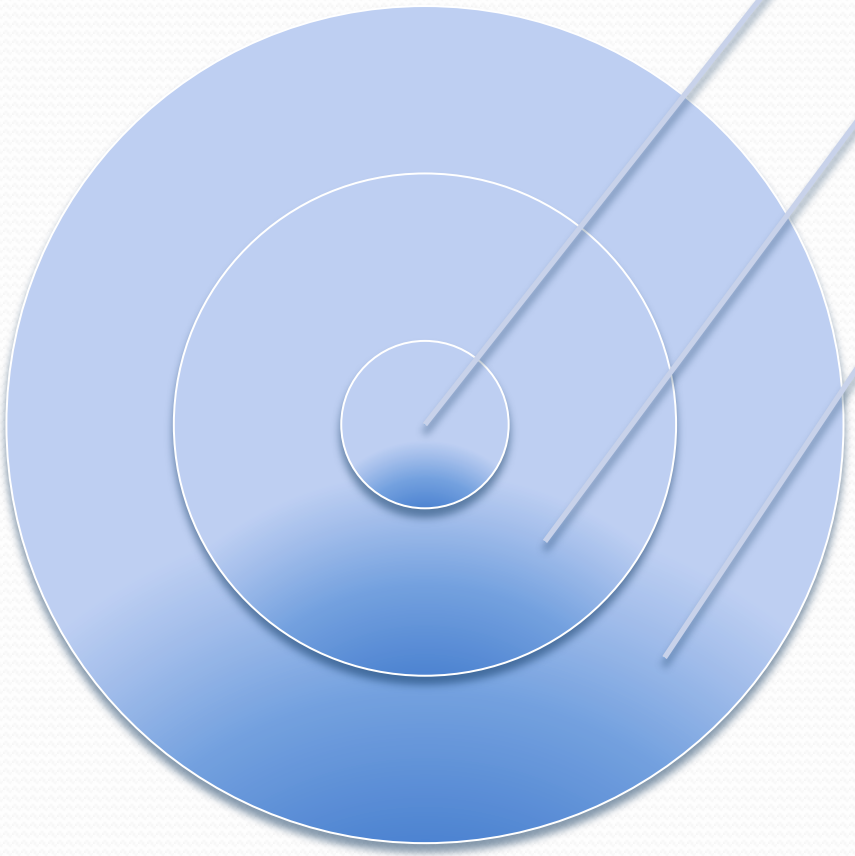
IDS Software

- Snort
- Barnyard2
- Pulled Pork
- stunnel

Packet capture

- TCPDump
- Daemonlogger

Management system



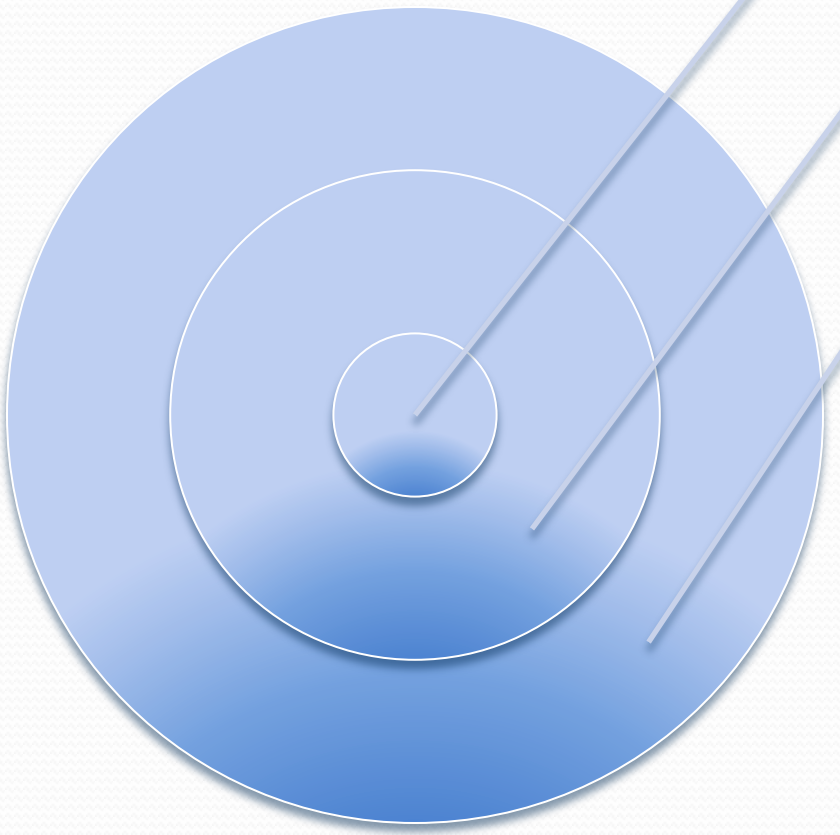
Secured OS

LAMP

Management Software

- BASE, Snorby, OCCIM, Splunk, Nagios, etc.

Analyst Systems



Secured OS

Management System Interface

Analysis tools

- Wireshark
- Tcpdump
- Netwitness

But I thought you wanted a secure system!

Lab

- Test system
  - Test rules on the IDS
  - Test Configuration changes
  - Can be used as a backup
- A safe environment to:
  - Play with malware
  - Try hacks

These activities can help you to discover the criteria to build custom rules for the IDS.

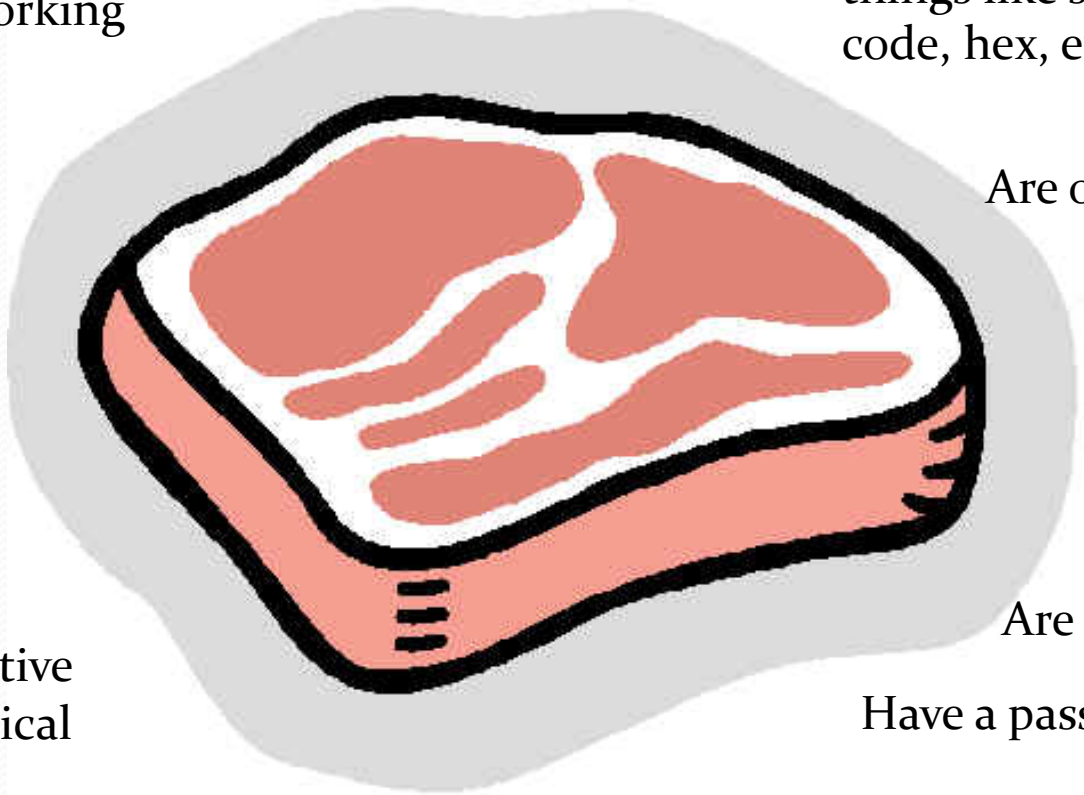
It's probably a good idea to use VM's for your lab.

Analysts (the meat of the operation)

- You need highly skilled people who:

Are comfortable with things like source code, hex, etc…

Know networking



Understand attacks

Are open to new ideas

Understand Malware

Don't blink

Don't ever call in sick

Are creative thinkers

Are good at deductive reasoning and critical thinking

Have a passion for this

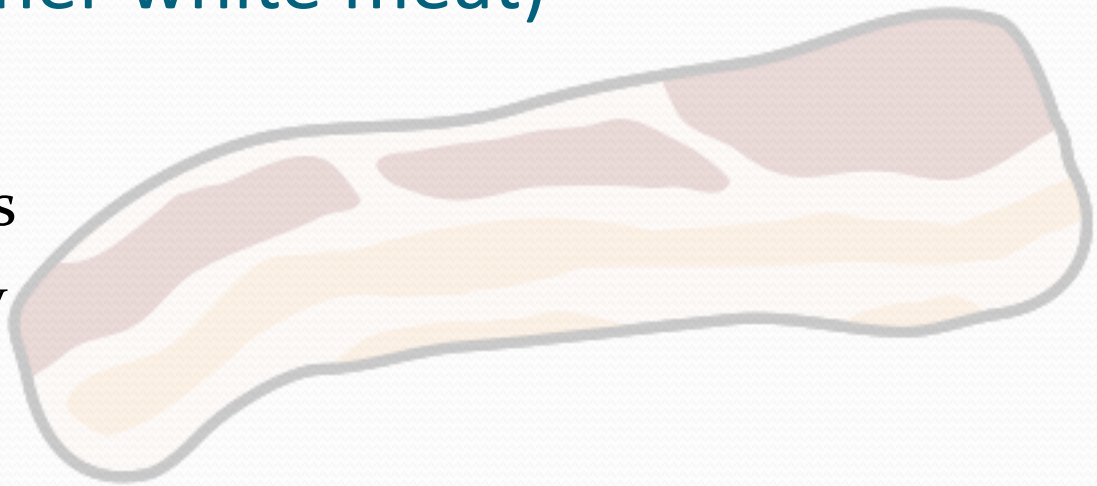
Love to keep learning

Don't need sleep

Other experts

- System/Network Administrators
  - Keep the whole thing working
  - Tune IDS rules
- Forensics Experts
  - For more in-depth analysis
- Incident Response
  - To mitigate incidents after they happen
- External entities
  - Government, law enforcement, etc…

Users (the other white meat)

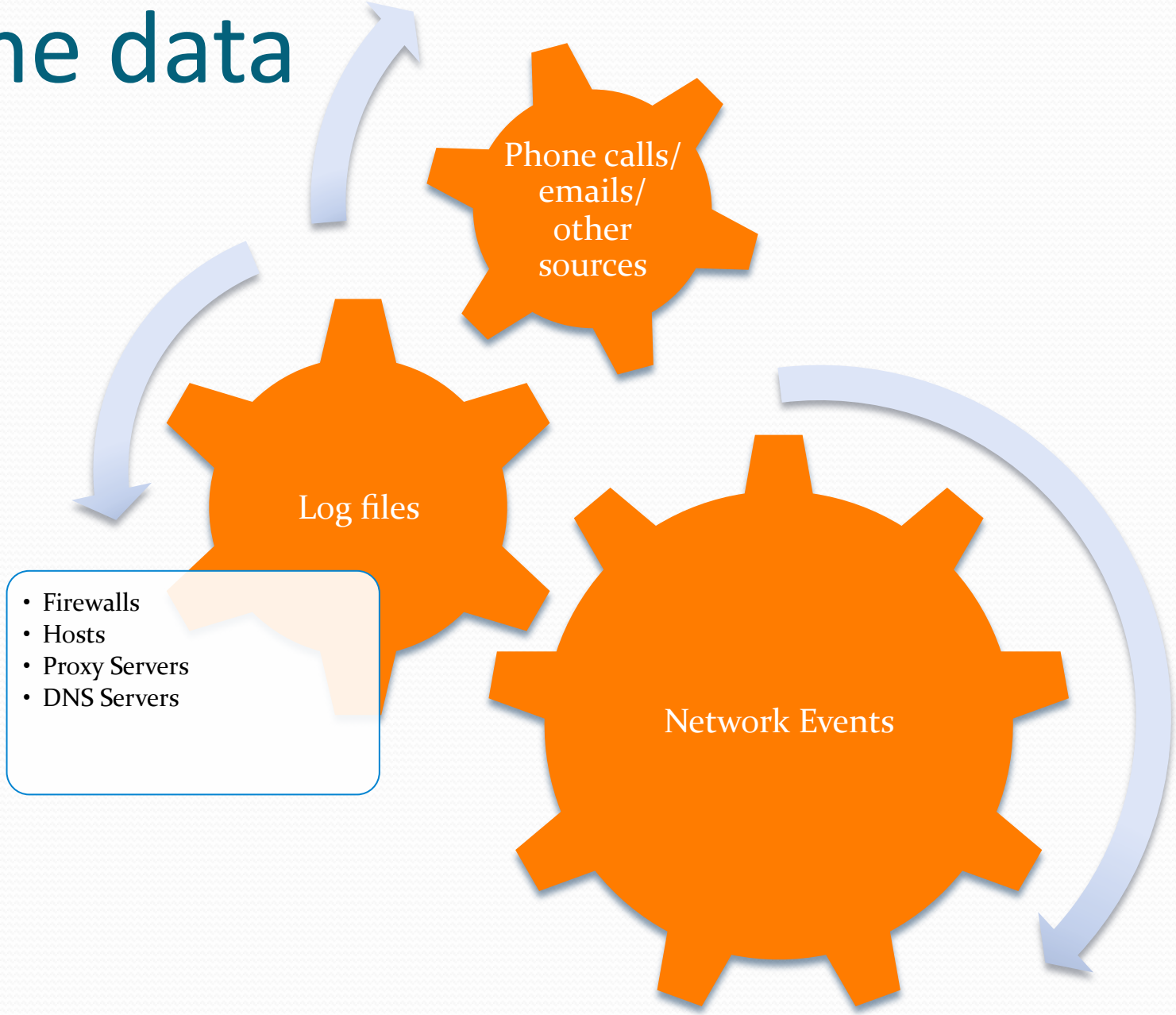


- Report things
  - Phishing emails
  - Stolen property
  - Loss of data
- Do things
  - Download malware
  - Engage in inappropriate activities
- The most widely deployed IDS you have
  - If “tuned” properly…

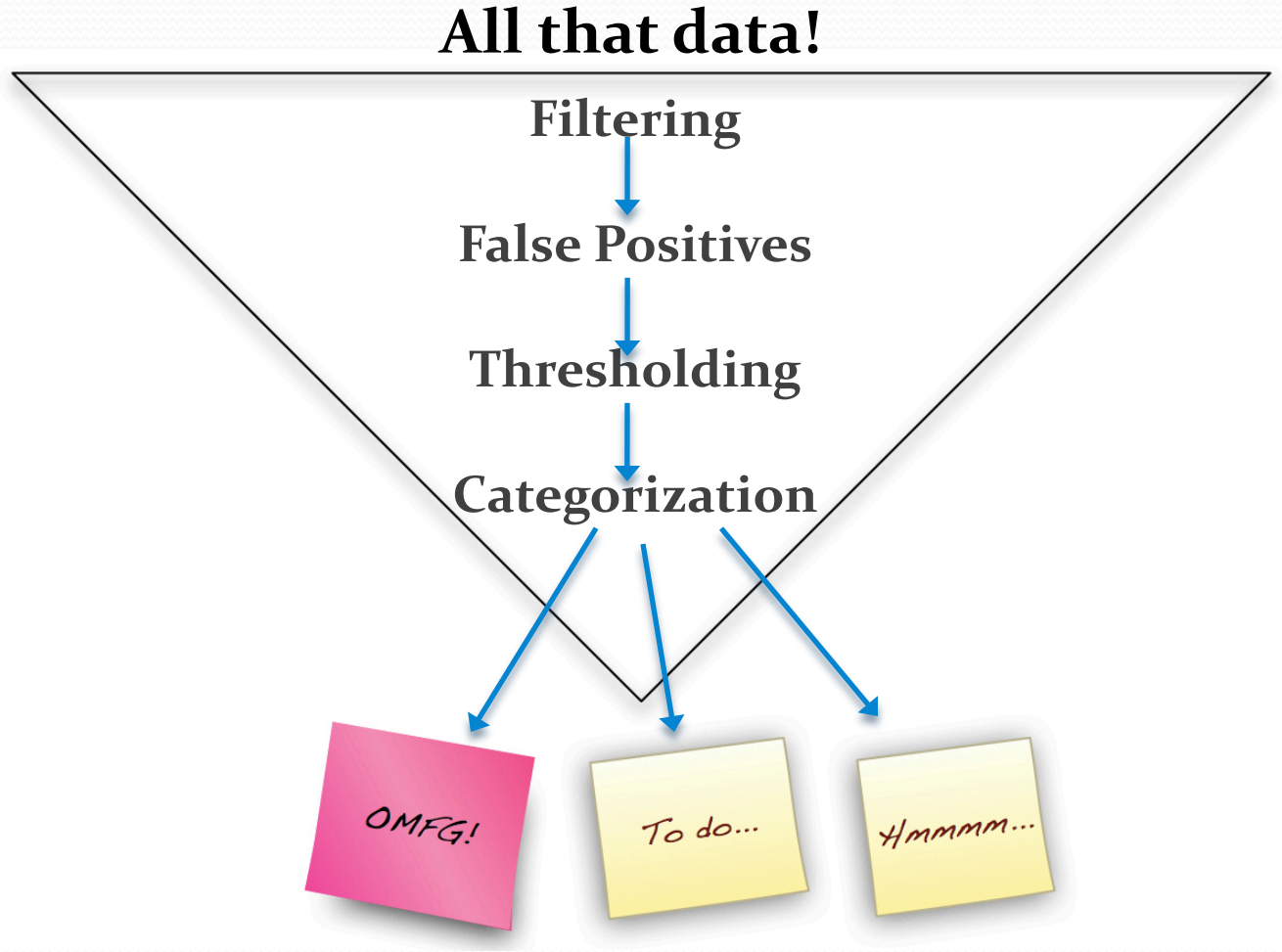
Management

- To interface with other entities
- Keep all the pieces from falling apart
- Make it rain (decide who gets the money)
- I guess someone has to make decisions…

The data


Phone calls/ emails/ other sources
Log files
Network Events
• Firewalls
• Hosts
• Proxy Servers
• DNS Servers

Handling all that data

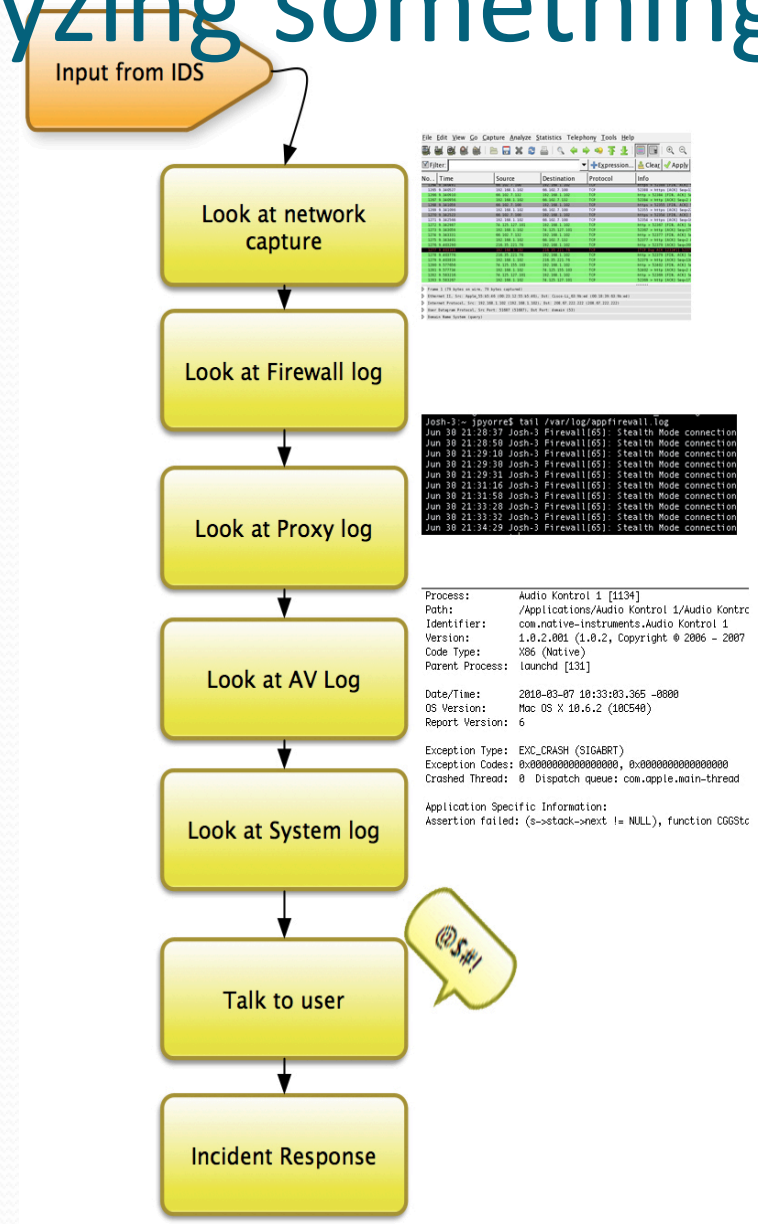


Categorization

US-CERT Recommends the following categories for events

Category	Name
CAT 0	Exercise/Network Defense Testing
CAT 1	Successful unauthorized Access
CAT 2	Denial of service
CAT 3	Successful installation or post-install beaconing of malicious code
CAT 4	Improper Usage
CAT 5	Scans/probes/Attempted Access
CAT 6	Investigation

Analyzing something like malware



Mitigation/Incident Response

- User education
- User access controls
  - Stop giving users administrative access
- Proxy servers and firewalls
  - Deny access to known bad sites
  - Deny certain kinds of downloads
  - Block posting to known bad IP's